

تجربة الجزائر في مكافحة الجريمة الإلكترونية

د.خضراوي الهادي*، د.بوقرين عبد الحليم**
كلية الحقوق والعلوم السياسية
جامعة عمار ثليجي
الاغواط، الجزائر

e.khadraoui@lagh-univ.dz, Halim.ma@yahoo.fr

الملخص— موضوع الدراسة،

الجرائم الإلكترونية، كل سلوك غير مشروع يتم بالتدخل في العمليات الإلكترونية التي تمس أمن النظم المعلوماتية والمعطيات التي تعالجها،... هذه الجرائم قلبت موازين التجريم والعقاب فلم يعد الأمر يتعلق بسلوك مادي ملموس وإنّما بأفعال في العالم الافتراضي، كما أنّ آليات التحقيق العادية لم تعد كافية فالأمر لا يتعلق بقوة بدنية أو مهارات قتالية.. وإنّما مدى معرفة المحقق بتقنية المعلومات وإتقانه لمتطلبات الإعلام الآلي والاتصالات، هو الذي يساهم في القبض على المجرم الإلكتروني .

في ظل تزايد الجرائم الإلكترونية وتنوّع أنماطها، وأساليبها وقفت الأجهزة المختصة بالبحث والتحقيق وعلى رأسها الضبطية القضائية عاجزة عن مواكبة هذا التطور، وملاحقة هذا النوع من الجرائم، وهو الأمر الذي دفع بالعديد من الدول في اللجوء إلى إنشاء أجهزة مختصة تستطيع التعامل مع هذا النوع من الإجرام.

سبب الدارسة:

يُواجه المشرّع مختلف الجرائم بالتجريم والعقاب كنوع من المكافحة الموضوعية، وفي سبيل ضبط هذه الجرائم والقبض على مرتكبيها يوفر المشرع الإمكانيات البشرية، والمادية اللازمة لذلك كنوع من المكافحة الإجرائية، والامر يبقى عاديا لا يثير أي إشكال ما دمنا بصدد جرائم تقليدية عادية، إلا أن الأمر يختلف إذا ما كنا بصدد جرائم غير عادية جرائم تقع في عالم افتراضي متطوّر.

إذا عجزت القواعد الموضوعية والإجرائية عن مواكبة هذا النوع من الإجرام ، وعليه جاءت هذه الدراسة التي تهدف إلى وضع حلول لتدخل القانون الجنائي في مجال العالم الافتراضي.

المنهجية المستخدمة:

في سبيل الوصول إلى النتائج والتوصيات المرجوة سوف نعتمد على المنهج التحليلي لمحاولة تحليل نزر من النصوص القانونية، وكذا المنهج الوصفي لمحاولة وصف الظاهرة الإجرامية، وبيان أبعادها، وبشكل أقل المنهج المقارن وخاصة ما تعلق منه باتفاقية بودابيست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

النتائج والتوصيات:

النتائج:

١. إنّ المشرّع الجزائري وفق إلى حد كبير وضع نصوص قانونية لمكافحة الجريمة الإلكترونية رغم أنه لم يسن قانون خاص لذلك.
٢. إنّ المشرّع الجزائري صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
٣. إنّ المشرّع الجزائري نص على قانون خاص ولا مثيل له في الدول العربية ،وهو القانون المتعلق بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها ،وهو قانون إجرائي وليس موضوعي.

التوصيات:

١. ضرورة المصادقة على الاتفاقية العربية لمكافحة الجريمة الإلكترونية .
٢. ضرورة التعاون الدولي في مجال توحيد النصوص التجريم في المجال الإلكتروني.
٣. ضرورة التعاون الدولي في مجال تكوين أجهزة مختصة في مكافحة الجريمة الإلكترونية.
٤. ضرورة استقطاب هذا النوع من المجرمين ومحاولة الاستفادة من خبراتهم.
٥. ضرورة اعتماد نظام المرشد الجنائي وفتح مواقع لتلقي الشكاوى لتسهيل عملية القبض على هؤلاء المجرمين.
٦. ضرورة تكثيف الدراسات حول طبيعة المجرم المعلوماتي، ونرى أنه حان الوقت لميلاد علم جديد وهو علم الإجرام المعلوماتي.

الكلمات المفتاحية—الإلكترونية، الافتراضي، الجريمة، الموضوعية، الإجرائية، المعلوماتية، نظام

* دكتوراه في القانون الخاص، عميد كلية الحقوق والعلوم السياسية.
رقم الهاتف : ٢١٣٦٦٩٧٣٦٣٤٠..

١. مقدمة

مرتْ المجتمعات البشرية بمراحل عديدة ومتنوعة ضمن مسارها الحياتي والمجتمعي، بدأت بمرحلة المجتمع الزراعي مروراً بالمجتمع الصناعي، فمرحلة المجتمع المعلوماتي لندخل بعد ذلك إلى حظيرة المجتمع الرقمي.... هذا الأخير الذي تمخض عن ثورة التكنولوجيا والإعلام، فغزت الحواسيب الآلية والانترنيت جميع مجالات الحياة، وأضحى استخدامها ضرورة لا غنى عنها بالنسبة للدول والحكومات ومؤسسات الدولة، ثم تطوّر الأمر ليصبح استعمال هذه التقنية متاحاً للأفراد وذلك من خلال تبادل المعلومات والمراسلات الخاصة وإبرام الصفقات التجارية، وبدأ عصر جديد امتزجت فيه التقنية بمختلف التصرفات المدنية التجارية والإدارية؛ وعلى الرغم من المزايا الكثيرة التي حملتها عملية امتزاج التقنية الرقمية بهذه التصرفات، وما وفرته من تكاليف وما حققته من رفاهية، إلا أنها لم تمر بسلام على المتعاملين بها فقد ظهر نوع جديد من الإجرام يعرف بالجرائم الإلكترونية أو المعلوماتية وهي جرائم تبدو غريباً نوعاً عن قواعد القانون الجنائي التقليدي.

الجريمة الإلكترونية دفعت بالكثير من التشريعات إلى التدخل من أجل حماية المصالح المتضررة منها، ومن هنا طفت إلى السطح عدة إشكاليات قانونية حول قدرة النص الجنائي التقليدي على الإحاطة بهذه المفاهيم والسلوكيات، وهو ما خلق عدة صعوبات وتحديات أرقت صانع التشريع وكانت السبب في جدل فقهي واسع، ورغم أنّ العديد من التشريعات لم تقف مكتوفة الأيدي وإنمّا حاولت إنقاذ القانون الجنائي وتحديثه، إلا أن هذه التدخل لم يكن على قدم المساواة، حيث نجد أن بعض التشريعات كانت سباقة في وضع سياسة جنائية موضوعية وإجرائية للحد من هذه الجرائم بينما أكتفت تشريعات أخرى بجانب معين من الحماية ومنها من تخلف عن الركب.

وتأتي هذه المداخلة كمحاولة للكشف عن **سياسة المشرع الجزائري في مكافحة الجريمة الإلكترونية؟ ومن ثمة معرفة مدى نجاعة هذه السياسة في الحد من هذه الجرائم ؟.**

وسنحاول من خلال هذه الورقة العلمية التطرق إلى تجربة المشرع الجزائري في مجال مكافحة الجريمة الإلكترونية عبر المحورين التاليين :

المحور الأول: المكافحة الموضوعية للجرائم الإلكترونيةفي التشريع الجزائري

المحور الثاني: المكافحة الإجرائية للجرائم الإلكترونية في التشريع الجزائري

المبحث الأول: المكافحة الموضوعية للجرائم الإلكترونية في التشريع الجزائري

إنّ وضع نصوص قانونية جنائية لمواجهة الجرائم المعلوماتية كان وليد جدل فقهي حول مدى قابلية النصوص الجنائية التقليدية لتشمل على هذا النوع من القيم الجديدة، وحقيقة الأمر أن الاتجاه الفقهي القائل بإمكانية ذلك لم يكتب له النجاح، لأنّ تبني هذه الأفكار سيؤدي إلى تشويه المبادئ المستقرة التي تقوم عليها تلك الجرائم، الأمر الذي سيؤدي بدوره لا محالة إلى وجود ثغرات قانونية، وهو ما جعل الفكر القانوني يستقر ويقتنع بضرورة وضع نصوص قانونية خاصة بهذه الجرائم.

وبما أنّه لا يمكن مواجهة الجريمة المعلوماتية[1] بدون توفير حماية كافية للمجال والنطاق الذي تتواجد فيه المعلومات، فقد حاول المشرع الجزائري مكافحة الجرائم الماسة بالأنظمة والبرامج المعلوماتية أو كما يحب أن يسميه المشرع بـ " أنظمة المعالجة الآلية للمعطيات"، ومن ثمة حماية المعلومات المتواجد في هذه الأنظمة[2].

1- نظرا لحداثة هذا النوع من الجرائم فقد توالت التعريفات الفقهية لتعريفها ومن بين هذه التعريفات من يرى أنها :

- "..كل شكل من أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي".
- "..أي جريمة يتطلب ارتكابها معرفة بتقنية المعلوماتية حيث يدخل في نطاقها كل فعل غير مشروع ويكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لإرتكابها ".
- "..أي اعتداء على معطيات أو بيانات أو برامج الحاسوب بالمحو أو التعديل أو الحذف أو التغيير أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها، ويتسبب هذا الاعتداء في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر.. أو قصد الحصول على كسب اقتصادي أو مادي بطريق غير مشروع"..... أنظر، أسامة أحمد المناعسة، جرائم الحاسب الآلي و الانترنيت، دار وائل، ط١، عمان، ٢٠٠١، ص٧٠ و ما بعدها.

ومن بين أهم التعريفات المتعلقة بالجرائم الماسة بمتطلبات التجارة الإلكترونية نجد التعريف التالي: "أي نشاط غير مشروع موجه لنسخ أو تغيير او حذف أو الوصول إلى معلومات مخزنة داخل الحاسب الآلي أو التي تحولت عن طريقه"..... أنظر، شول بن شهرة، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، جامعة محمد خيضر بسكرة، ٢٠٠٩/٢٠١٠ ، ص٨٧.

2- ومن بين التشريعات العربية التي نصت على هذه الجرائم نجد المشرع القطري حيث جاء في المادة ٦٧ من قانون المعاملات والتجارة الإلكترونية رقم ١٦ لسنة ٢٠١٠م أنه يعاقب كل من تعمد الوصول بصفة غير شرعية إلى أي نظام معلومات أو رسالة بيانات أو خدمة تجارة الكترونية أو معاملة ذات صلة بما في ذلك تجاوز الإجراءات التقنية الأمنية وذلك قصد الحصول على معلومات أو استخدام آخر غير مشروع لنظام المعلومات أو رسالة البيانات أو خدمة التجارة الإلكترونية أو معاملة ذات صلة.... في حين نجد أن المشرع الإماراتي لم يشر إلى هذه الجريمة بوضوح لكنه نص على تجريم كل من ارتكب فعلا يشكل جريمة بموجب التشريعات النافذة باستخدام وسيلة الكترونية ينظر، المادة ٢٩ من قانون المعاملات و التجارة الإلكترونية الإماراتي رقم ١ لسنة ٢٠٠٦.

المطلب الأول: الحماية الجنائية للبرامج والأنظمة

لقد تنبه المشرّع الجزائري إلى خطورة المساس بالأنظمة والبرامج فعمد إلى تجريم هذه الأفعال بموجب تعديل قانون العقوبات بالقانون رقم ٠٤/٠٩، في المواد من ٣٩٤ مكرر إلى ٣٩٤ مكرر٧ تحت عنوان **"المساس بأنظمة المعالجة الآلية للمعطيات"**.

وتجدر الإشارة إلى أن المشرع الجزائري قد صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1] بتاريخ ٠٨ سبتمبر ٢٠١٤ وقد جرمت هذه الاتفاقية المساس بالبرامج والأنظمة في المواد ٧ و٨ و٩ منها.

وبالرجوع إلى النصوص القانونية السالفة الذكر نجد أن المساس بأنظمة المعالجة الآلية للمعطيات يأخذ عدة صور تتغير بتغير السلوك المرتكب نتناول هذه الصور فيما يلي.

الفرع الأول: تجريم الدخول إلى نظام المعالجة أو البقاء فيه بصفة غير شرعية

لقد نتج عن ربط الحاسبات الآلية ببعضها عن طريق شبكة اتصال يؤدي إلى سرعة انتقال وتداول المعلومات والبيانات الأمر الذي يؤدي إلى اختصار الزمن وهو ما يبحث عنه **المتعامل الإلكتروني**، بيد أن هذا الأمر سهل من عملية التطفل على تلك المعلومات أو البيانات الأمر الذي يؤدي في النهاية إلى قرصنتها والسطو عليها، حيث تستهدف هذه الجرائم المؤسسات المصرفية وشركات التأمين والشركات الخاصة أو مؤسسات القيم المالية مواقع التجارة الالكترونية[2].

وقد استشعر المشرّع في عديد الدول إلى الحاجة لإدخال تشريعات جديدة تحمي المعلومة[3] داخل نظام الكمبيوتر، نظراً لقصور القواعد التقليدية في قانون العقوبات عن حماية هذا النظام، فوجدت عدة نصوص تجريمية تعاقب على مجرد الدخول في نظام الحاسب الآلي فضلا عن إتلاف المعلومات المبرمجة أو الموجودة داخل هذا النظام[4].

أولا: الدخول إلى نظام المعالجة

جاء في المادة ٣٩٤ مكرر من قانون العقوبات أنه "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من ٥٠,٠٠٠دج إلى ١٠٠,٠٠٠دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..."[5] ويتضح من هذه المادة أن الركن المادي لهذه الجريمة يتكون من عنصرين هما الدخول إلى نظام المعالجة أو البقاء فيه بعد الدخول وسنتناول هذين العنصرين بشيء من التفصيل.

يتحقق الدخول بالولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام[6]، وقد حصل نقاش واسع في الولايات المتحدة الأمريكية حول عبارة " الدخول " وذلك سنة ١٩٩٦ أمام محكمة كانساس العليا في قضية allen حيث حاولت التضييق من مفهوم الدخول[7]، ويقوم هذا السلوك المجرم عن طريق قيام الجاني الإلكتروني بإختراق أنظمة وبرامج الحاسوب ويمكن أن يتصور الدخول إلى هذه الأنظمة بعدة فرضيات نذكر منها:

1- صادق المشرع على هذه الإتفاقية بموجب المرسوم لرئاسي رقم ٢٥٢/١٤ بتاريخ ٨ سبتمبر ٢٠١٤ الجريدة الرسمية رقم ٥٧.

2- أنظر، سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية، ط١، ٢٠١١، ص٣١٨.

3- تبرز حاجة المعلومة الإلكترونية إلى الحماية بالنظر إلى أهميتها بالمقارنة مع المعلومات داخل الملفات الورقية.. كما تتميز المعلومة الإلكترونية بالضخامة والتنوع، بل منها ما يتعلق بالحياة الخاصة للأفراد ومنها ما يتعلق بالأمن القومي... أنظر، أكثر تفاصيل شيماء عبد الغني محمد عطالله، الحماية الجنائية للتعاملات الالكترونية، دار الجمعة الجديدة، ٢٠٠٧، ص٩٤.

4- ويعتبر البعض أن القانون السويدي لسنة ١٩٨٣ أول قانون يعاقب على الدخول في نظام الحاسوب بصفة غير شرعية، ثم تليه عدة تشريعات أخرى ومن ذلك القانون الألماني و قانون ولاية فرجينيا في الولايات المتحدة الأمريكية والقانون الكندي والنمساوي والياباني ثم انتقل الأمر إلى التشريعات العربيةكالقانون التونسي والقطري..الخ أنظر، شيماء عبد الغني محمد عطالله، المرجع السابق، ص٩٥.

5- وهو ما نصت عليه الإتفاقية العربية لمكافحة الجريمة المعلوماتية حيث جاء في المادة ١/٦ منها "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

6 – حيث تشير المذكرة التفسيرية لإتفاقية بودابيست أن الولوج غير القانوني يجب أن يكون دون حق وذلك يعني ألا عقاب على الولوج المصرح به أو كان الولوج متاحا للجمهور.. أنظر أكثر تفاصيل... هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ٥٤ وما عدها.

7- وتتلخص وقائع القضية في قيام المتهم allen بإستخدام حاسبه الآلي للإتصال بحاسب شركة الهاتف الجنوبية الغربية التى تتحكم في تحويل الإتصالات البعيدة المدى، حيث تلاعب المتهم بنظامها بطريقة تسمح بالإتصال الهاتفي مجاناً، وقد إتضح للمحققين أن allen إخترق النظام عن طريق فك كلمته السرية، ومن ثمة إزالة الدليل على نشاطه بإلغاءه للسجلات.. وقد دافع المتهم عن نفسه أمام المحكمة بأنه لا يوجد دليل على دخوله إلى الحاسب الآلي للشركة، إلا أن الإدعاء إعتمد على تعريف التشريع الواسع لعبارة "الدخول access " والتى تقر بأن الدخول يعني الإقتراب أو إصدار أمر أو الإتصال بـ.أو أية أشياء أخرى تؤدي إلى إستخدام مصادر الحاسب الآلي... لكن المحكمة أجابت بأن هذا التعريف كان واسعا بحيث يؤدي إلى القول بعدم دستورية التشريع لغموضه.. وإنتهت المحكمة إلى أن المعنى الكامل والعادي يجب أن يطبق عوضا عن الترجمة المشوهة للتعريف المتوافر.... وأن القول بأن دخول المتهم إلى النظام يظهر في قيامه بالبحث عن كلمة العبور الخاصة بنظام الشركة المذكورة للوصول إلى المعلومات قول لا دليل عليه، وهو ما يؤدي إلى القول بعدم دخول المتهم إلى حاسابات الشركة أنظر، خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، ٢٠١٠/٢٠١١، ص ١٤٠ وما بعدها.

- الدخول عن طريق تشغيل حاسب آلي مقفول: حيث يقوم الجاني في هذه الحالة بفتح جهاز الكمبيوتر وتشغيله ثم يدخل إلى النظام.. غير أن العبرة ليست بتشغيل الكمبيوتر ولكن بالتمكن من الدخول إلى النظام إذ يستطيع الجاني أن يدخل إلى النظام والجهاز مغلق، وقد يتمكن من تشغيل الجهاز دون أن يصل إلى الملفات ويمكن اعتبار هذه الحالة شروعا ويعاقب عليه... **لكن الإشكالية تثار فيما لو كان النظام مفتوحا وقام الجاني بالإطلاع عليه عن طريق شاشة الجهاز؟..** يرى البعض أنّ مجرد الإطلاع على تلك المعلومات الظاهرة على شاشة الجهاز لا يعد دخولاً للنظام، إنما يكون الدخول إذا كان الجاني هو من قام بتشغيل الجهاز والولوج إلى النظام[1].

- استعمال حاسب آلي مفتوح: في هذه الحالة يكون جهاز الحاسوب قيد الاستعمال ثم قام الجاني باستغلال ذلك ودخل إلى إحدى أنظمة المعالجة أو الملفات المتواجدة فيه.. وعليه فإن ذلك يعد دخولاً غير مشروع ويعاقب عليه.

- الاختراق: في هذه الحالة يتمكن المتهم من الدخول إلى الكمبيوتر المربوط بحواسيب أخرى أو بشبكة خاصة أو بالانترنيت.. عن طريق جهازه الخاص باستخدام وسائل تقنية حديثة كبرامج التجسس والاختراق وهو أمر يتطلب مهارة عالية ويعرف الجناة من هذا النوع بالهاكرز.. الخ.

وفي سابقة قضائية فريدة من نوعها قضت محكمة باتنة[2] بتاريخ ٢٠١٠/٠٦/٠١ في قضية تتعلق بإختراق نظام المعالجة، وتتلخص وقائع القضية في أنه بتاريخ ٢٠٠٩/٠٤/٨٠ قام شاب جزائري بإرسال رسالة بريدية لمؤسسة أمريكية تدعى صاقونات وركس sago net works وهي تعد بنك للمعلوماتية بولاية فلوريدلا، يدعي من خلالها أنه اكتشف طريقة للدخول إلى المعطيات الإلكترونية للمؤسسة المذكورة، وأن جميع المعطيات والمعلومات الخاصة بالشركة قد تم استنساخها، ليقوم الجاني بعد ذلك بإرسال رسالة اخرى يطلب فيها مبلغا ماليا ... وبعد البحث والتحري من طرف الضبطية الجزائرية تم تحديد هوية المتهم الذي قام بالاختراق، حيث اعترف بإختراقه لعدة مواقع إلكترونية عن طريق القرصنة باستعمال الخط الهاتفي لمنزله مستعينا بشبكة الانترنيت للمتعامل "فوري"، وكذا استعمال عدة عناوين إلكترونية وهمية، كما صرح بحصوله على مبالغ مالية من هذه العمليات، وقد قضت المحكمة عليه بالحبس عاما نافذا و٥٠,٠٠٠ دج غرامة مالية[3]"..

- الدخول بإستعمال خطوط الاتصالات: وفي هذه الحالة يعمد الجاني إلى العبث بخط من خطوط الهاتف المتصل بالنظام محل الجريمة من أجل إعطاء تعليمات إلى هذا النظام لتحقيق غرض معين كالإطلاع على شروط صفقة معينة أو بيانات المشترين والبائعين...[4].

- الدخول إلى نظام الحاسب الآلي باستعمال بطاقة الغير: ويتم ذلك عند قيام الجاني باستعمال بطاقة الغير للدخول إلى نظام الكمبيوتر التابع لإحدى الجهات من أجل الحصول على أمر معين أو بيانات معينة أو معلومات هي مقتصرة على أصحاب البطاقات[5].

هذا ويثير بعض الباحثين إشكالية تتعلق **بطبيعة الدخول الذي يتم عن طريق إلتقاط الإشعاعات والإشارات الصادرة عن الكمبيوتر ومدى خضوعه لهذه الجريمة ؟..** حيث يعتبر هؤلاء أن الدخول بهذه الطريقة يعد تداخلاً و ليس دخولاً... وما يعزز هذه الإشكالية أن كثيراً من القوانين جرمت السلوكين معاً " التداخل والدخول " ومن ذلك ما نص عليه قانون جرائم الكمبيوتر في ولاية تينيسي Tennessee الأمريكية حيث عاقب كل من يتداخل أو يسبب تداخل الغير أو يحاول التداخل - مع علمه بذلك - في برامج كمبيوتر أو البيانات التي يحتويها أو في نظام الكمبيوتر أو شبكته..."[6].

1- وما تجدر الإشارة إليه أن الدخول لا يكون محققا إذا كان برضا صاحب النظام.. لذلك يعتبر البعض أن عدم الرضا ركن في هذه الجريمة فإذا توفر الرضا انتفت الجريمة حتى ولو استعمل الجاني النظام في غير الأغراض التي أرادها صاحب النظام... أنظر، شيماء عبد الغني محمد عطاالله، المرجع السابق، ص١٠٨... أنظر أيضا، عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤، ص٣٠.

2- ولاية تقع شرق الجزائر.

3- أنظر، حكم محكمة باتنة رقم ٠٥٢٧٢/١٠، الصادر بتاريخ ١٠-٠٦-٢٠١٠.. أنظر أيضا خليفة محمد، المرجع السابق، ص ٢٠.

4- وقد تم اتهام مهندسين يعملون في شركة اتصال فرنسية لاستعمالهم خط التليفون المركب على أجهزة عارضة للألعاب الالكترونية... وتمكنوا من جراء ذلك من الحصول على جوائز على اعتبار أنهم فازوا بالألعاب التي قاموا بها... في حين أنهم تحايلوا على الجهاز الخاص باللعبة وتحصلوا على معلومات ساعدتهم على الفوز... أنظر، شيماء عبد الغني محمد عطاالله، المرجع السابق، ص١٠٨.

5- وقد قضي في فرنسا بوقوع هذه الجريمة على من استخدم بطاقة السحب مع الرقم السري الخاص بشخص آخر دون موافقته وعد ذلك من قبيل الدخول أنظر تفاصيل أكثر.. محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٣، ص١١٥٠.

6- ومن الوسائل المستعملة في هذا المجال أيضا نجد أسلوب "التخفي Déguisement"، ويقصد انتحال صفة من له الحق في الدخول إلى النظام.... غير أن أخطر وسيلة تعرف بالقناة المتخفية "canal cache"، وهي طريقة جد معقدة يعمد فيها الجاني لاختراق نظام الحماية المعتمد من طرف صاحب النظام.. ومن الجناة الالكترونيين من يعتمد على وسيلة التسلل "Faufilement" وتتم عن طريق تتبع مستعمل رخصة الدخول إلى النظام.

وعليه فإن الدخول بهذا المفهوم يختلف عن التقاط الإرسالات أو الإشارات عن بعد.. ذلك أن المتهم لا يدخل إلى نظام معين، لذلك يرى البعض ونحن نميل إلى رأيهم أنه يجب تخصيص نص يعاقب على التلصصوالتجسس على تلك الرسائل والبيانات المرسلة..، وهو ما أشارت إليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية والتي صادق عليها المشرع الجزائري حيث نصت المادة ١/٠٦ منه على عبارة " وكل اتصال غير مشروع".

وكذا ما جاء في المادة ٠٧ منها والتي "الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات".

ومن خلال التبيان السابق لعنصر الدخول إلى نظام المعالجة الآلية للمعطيات بصفة غير شرعية يتضح أن هذه الجريمة تقع بمجرد إتيان النشاط فمجرد الدخول يعد جريمة بغض النظر عن الأفعال اللاحقة له[1].

ثانيا: البقاء غير المشروع داخل نظام المعالجة

يكون هذا السلوك المجرم متحققا بتواجد الجاني داخل النظام المعلوماتي بدون رضا من له الحق في التحكم فيه[2]، ويكون ذلك إما بعد الدخول غير المشروع في النظام، أو في حالة البقاء داخل النظام بعد نفاذ الوقت المحدد للبقاء داخله، وكثيرا ما يحدث ذلك إذا كان استعمال النظام بمقابل محدد بمدة زمنية.. وهو ما جعل البعض يطلق على هذا الفعل المجرم بسرقة وقت الآلة[3]، وقد تتحقق جريمة البقاء داخل النظام دون جريمة الدخول وذلك في الحالة التي يكون فيها الدخول إلى النظام عن طريق الخطأ أو الصدفة[4]، ومحل التجريم في هذه الحالة هو بقاء الجاني داخل النظام، إذ كان يجب عليه في هذه الحالة أن يقطع وجوده وينسحب فوراً[5].

نشير أنه يكفي لتحقق عنصر البقاء مجرد التواجد داخل كل أو جزء من النظام ولا يشترط أن يضاف إليه التقاط المعلومات أو محوها أو إتلاف بل مجرد التجول يكفي لقيام هذا السلوك المجرم[6]..

جريمة الدخول إلى نظام المعالجة الآلية للمعطيات أو البقاء فيه من الجرائم العمدية التى تقوم بتوافر القصد الجنائي العام بعنصرية العلم والإرادة، حيث يتوجب أن يكون الجاني عالما بعدم أحقيته في دخول النظام أو البقاء فيه، وأن هذا الفعل مخالف لإرادة صحاب النظام، ومع ذلك يقدم على دخول النظام أو البقاء فيه[7].

وبالرجوع إلى نص المادة ٣٩٤ مكرر السالفة الذكر نجد أن المشرع يشترط أن يتم الدخول أو البقاء بطريقة الغش "...كل من يدخل أو يبقى عن طريق الغش"، ويقصد بطريق الغش سوء نية الجاني بحيث يعلم بأن دخول النظام أو البقاء فيه ليس من حقه ومع ذلك يقدم على ذلك، ويستخلص سوء النية في غالب الأحيان من اختراق الجاني لنظام الحماية الخاص بنظام المعالجة، وبالنسبة لعنصر البقاء فيستنتج من خلال العمليات والتصرفات التى قام بها الجاني داخل النظام[8].

من خلال تحليلنا للنص المتعلق بجريمة الدخول والبقاء غير الشرعي في نظام المعالجة نلاحظ أن المشرع قد أحسن صنعا في صياغة هذه المواد ولكن ما يعاب عليه هو عدم النص على فعل التداخل الذي يختلف عن

ولهذا يعد الدخول بهذه الوسيلة تهديدا حقيقيا لأمن المعلومة ويخلق العديد من المشاكل التقنية، حيث يؤدي إلى هدم بيانات سرية مثل كلمة المرور ومعلومات سرية خاصة بالبرنامج.... ينظر، التقرير التفسيري لاتفاقية بودابست المتعلقة بجرائم الكمبيوتر خاصة المواد ٣ إلى ٦ في. هلالي عبد الإله أحمد، المرجع السابق ص ١٨ وما عدها.

1- فبمجرد الدخول إلى النظام المعلوماتي تقوم الجريمة حتى لو لم يترتب على فعل الدخول ضرر، أو لم يحقق الجاني فائدة من الدخول سواء كان الدخول إلى النظام كله أو جزء منه.. كما يعد مرتكبا للسلوك المجرم كل شخص مسموح له بالدخول إلى جزء معين من النظام لكنه تعداه أجزاء أخرى.... أنظر، علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة والنشر، بيروت، ١٩٩٩، ص١٣٠-١٣٣.

2- أنظر، رامي عبد الحليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجموعة الملتقى الدولي حول التنظيم القانوني للانترنيت.... مجلة دراسات، ٢٠٠٩، ص١٧.

3- أنظر، شيماء عبد الغني محمد عطالله، المرجع السابق، ص١٢١.... أنظر أيضا أمال قارة، المرجع السابق، ص١١١.

4- ويرى البعض أن هذه الجريمة كثيرا ما تتحقق من طرق العاملين في الشركات والمؤسسات الذين يبقون في النظام مع أن الوقت المحدد لهم قد انتهى، وبالتالي فإن تجريم البقاء داخل النظام هو موجه إليهم بالدرجة الأولى فاستعمال النظام بعد انتهاء الوقت المحدد يعد دخولا وبقاء في النظام، غير أن أحكام القضاء الفرنسي في هذا المجال تؤكد على ضرورة توافر القصد الجنائي.. وهو البقاء في النظام بغرض استعمال في أغراض شخصية للمتهم، فمستخدموا الشركات الذين يستعملون أجهزة الحاسوب غالبا ما يستعملونها في ألعاب التسلية الأمر الذي يكلف الشركة مبالغ طائلة نظير استعمالهم لخطوط الهاتف... ينظر، شيماء عبد الغني محمد عطالله، المرجع السابق، ص١٢٤.

5- أنظر، أمال قارة، الحماية الجنائية للمعلوماتي في التشريع الجزائري، دار هومة للنشر، ط ٢٠٠٧، ص١١٠.

6- أنظر، علي عبد القادر القهوجي، المرجع السابق، ص١٣٤-١٣٦.

7- أنظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام التجارة الالكترونية ، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤، ص٣٥٠.

8- لذلك يرى أغلب الفقه أن الدخول يكون مشروعا متى كان بطريق الصدفة أو السهو أو الخطأ، وما على الشخص في هذه الحالة إلا أن يخرج من فوره، فإذا أبى ذلك توافر في حقه القصد الجنائي وظهرت نية الغش لديه، كما لا يتوفر القصد الجنائي إذا كان دخول الجاني أو بقاؤه مسموح به أصلا أو وقع الجاني في خطأ بشأن حقه في الدخول أو البقاء سواء من حيث النطاق أو الزمان.

ويمكن للقاضي أن يستدل على توفر القصد لدى الجاني بعدة قرائن كاستعمال برامج للاختراق أو ضبط المعطيات المتحصلة نتيجة الاختراق بحوزته، وهو ما استدلت به محكمة باتنة في حكمها السالف الذكر حيث جاء فيه" حيث انه ثبت للمحكمة من خلال اوراق القضية لاسيما الخبرة الفنية الخاصة بتحليل البريد الإلكتروني للمتهم ..أنه كان يقوم بالدخول عن طريق القرصنة " الغش" باستعمال برامج متنوعة.. .

فعل الدخول داخل النظام... هذا من جهة ومن جهة أخرى نلاحظ أن عقوبة الحبس من ثلاثة أشهر إلى سنة وغرامة مالية من ٥٠,٠٠٠ دج إلى ١٠٠,٠٠٠دج، تبدو غير كافية لردع هذه الجريمة خاصة في مجال المعاملات التجارية الإلكترونية التى تقوم على الثقة والأمان في معاملاتها... لذلك نقترح أن يكون النص على النحو التالي : "يعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة مالية من ٥٠,٠٠٠ دج إلى ٥٠٠,٠٠٠ دج كل من يدخل أو يتداخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..." .

الفرع الثاني: تجريم المساس بسير نظام المعالجة

تأتي هذه الجريمة كتكملة لجريمة الدخول أو البقاء في النظام حيث يؤدي فعل الجاني إلى إحداث تغييرات داخل عمل النظام مما يؤدي إلى تعطيل سيره أو الإخلال بكيفية تشغيله، وهو السبب الذي جعل المشرع يشدد العقوبة حيث جاء في المادة ٣٩٤ مكرر في فقرتها الثانية أنه "...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من ٥٠,٠٠٠دج إلى ١٥٠,٠٠٠دج"[1].

وهو ما نصت عليه الاتفاقية العربية السالفة الذكر في نص المادة ٢/٦ منها حيث جاء فيها " تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

ب) الحصول على معلومات حكومية سرية".

وعليه فإن هذه الجريمة تتحقق بالأفعال التالية :

- الإخلال بسير نظام المعالجة عن طريق الحذف: أي أن يحدث الجاني نقص في معطيات النظام عند محاولته في الدخول إليه، ولا يشترط أن ينصب الحذف على جميع المعطيات المتعلقة بنظام المعالجة وإنما يكفي أن يحدث حذف جزئي لها[2].

- الإخلال بسير نظام المعالجة عن طريق التغيير: يفترض التغيير استبدال معطيات مكان أخرى نتيجة الدخول أو البقاء في النظام، فيبقى النظام في هذه الحالة سليما لكن بوجود معطيات مغايرة، ولا يشترط في هذه الحالة أيضا تعطيل النظام أو فساده إنما مجرد التعديل يجعل السلوك المجرم قائما[3].

- التخريب: يعني فعل التخريب أن يترتب على دخول الجاني أو بقاؤه داخل النظام إتلاف نظام اشتغاله وبالتالي تعطيله عن أداء مهامه، ويتضمن التخريب أو الإتلاف العبث في معطيات النظام المتعلقة بنظام تشغيله بصورة لا يمكن إصلاحها... ففعل التخريب أخطر من فعل التغيير غير أن المشرع ربط بين فعل نتيجة التخريب ونظام اشتغال المنظومة وبالتالي تعطيل النظام، فإذا ترتب عن دخول الجاني أو بقاؤه داخلا النظام نوعا من التخريب الذي لا يؤدي إلى تعطيل نظام اشتغاله فلا ظرف تشديد.

تجدر الإشارةإلى أنظروف التشديد سواء كانت حذفا أو تغييرا أو تخريبا ليست أفعال مستقلة بذاتها وإنما مرتبطة بجريمة الدخول أو البقاء داخل النظام.. وتعتبر ركنا في هذه الجريمة إذ أن الأفعال المذكورة سابقا ليست عمدية.

وتعتبر هذه الجريمة ليست جريمة عمدية ففعل الحذف أو التغيير أو التخريب أفعال غير إرادية للجاني وإنما وقعت نتيجة دخوله أو بقائه في النظام... ومع ذلك يمكن للجاني أن يدفع المسؤولية عن نفسه بأن يثبت أن الحذف أو التغيير أو التخريب يرجع لسبب آخر أو قوة قاهرة [4].

1- والملاحظ أن المشرع الجزائري اكتفى بالنص على هذه الجريمة كظرف تشديد لجريمة الدخول أو البقاء في نظام المعالجة، في حين نجد المشرع الفرنسي نص على هذه الجريمة كظرف تشديد وكذا بصفة مستقلة في المادة ٢/٣٢٣ من قانون العقوبات الفرنسي إذا كانت بالعمد.

2- ولكن الإشكال المثار هنا هو هل يشترط أن يؤدي هذا الحذف إلى تعطيل النظام؟... بالرجوع إلى نص المادة المذكور سالفا نجد أن المشرع لم يشترط أن ينتج عن هذا الحذف تعطيل أو ضرر للنظام وبالتالي فمجرد وقوع حذف في معطيات المنظومة كاف لتشديد العقوبة.

3- ومن بين الإشكالات المثارة بهذا الشأن هي هل تقع الجريمة إذا كان من شأن هذا التغيير أن يؤدي تحسين سير النظام؟.... لا شك أن تجريم الدخول أو البقاء داخل نظام المعالجة هو تجريم وقائي حتى لا يحدث تعطيل لهذا النظام أو المساس بالمعطيات الموجودة فيه، والدخول إلى النظام أو البقاء فيه الذي يترتب عليه تحسين أداء عمل هذا النظام لا تعطيله يجعل من علة تجريم المساس بسير النظام غير متوفرة، ولكن هذا لا يعني انتفاء الجريمة فهذا التفسير قد لا يستقيم مع مبادئ القانون الجنائي حيث أن النص ذكر مصطلح "تغيير" ولا يهم بعدها أحدث تعطيل للنظام بسبب هذا التغيير أو تحسن أداؤه، غير أن البعض يرى خلاف ذلك ويذهب إلى أن جريمة الدخول أو البقاء في صورتها المشددة تتحقق إذا نتج عن التغيير أو الحذف أو الإتلاف تعطيل لسير النظام أو عدم قدرته على أداء وظائفه بأكمل وجه أنظر، شول بن شهرة، المرجع السابق، ص٩٥.

4- أنظر في هذا المعنى، أمال قارة، المرجع السابق، ص١١٤.

الفرع الثالث: جريمة المساس العمدي بسير نظام المعالجة وحاجة التشريع الجزائري لها

تعتبر هذه الجريمة من اكثر الجرائم الإلكترونية انتشارا ورغم أهمية هذه الجريمة إلا أنّ المشرّع لم ينص عليها صراحة، في حين نص عليها المشرع الفرنسي ضمن المادة ٢/٣٢٣ من قانون العقوبات الجديد، والتي جاء فيها أنه يعاقب على الأفعال التي تعوق أو تخل بسير نظام المعالجة الآلية للمعطيات أو البيانات بالحبس لمدة لا تزيد عن خمس سنوات والغرامة التي لا تزيد عن ١٠٠,٠٠٠ أورو...، وهو ما نصت عليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية في مادتها ٨. حيث جاء فيها "... تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق".

ويهدف الجاني من وراء هذه الجريمة تعطيل سير نظام المعالجة أو جعل هذا النظام غير قادر على أداء مهامه بصورة جيدة، ويتخذ الجاني في ارتكاب جريمة عدة أساليب وأفعال ولكنها لا تخرج عن الإعاقة[1] أو الإخلال[2].

وما تجدر الإشارة إليه أن كثير من شراح قانون العقوبات الفرنسي يصفون الأفعال المكونة لهذه الجريمة بأنها "عرقلة أو إعاقة" وفي الحقيقة هذا الوصف لا ينطبق تماما مع مضمون الجريمة، فالعرقلة أو الإعاقة قد تكون في شكل تبطيئ عمل النظام فقط...، والمقصود من هذه الجريمة هو إيقاف عمل النظام وبالتالي فإن المصطلح المناسب هو **"تعطيل عمل النظام"**.

وعلى عكس التعطيل أو التعديل أو التخريب الذي يلحق نظام المعالجة الآلية للمعطيات جراء الدخول أو البقاء فيه بصفة غير شرعية، فإن هذه الجريمة تتطلب أن يكون التعطيل أو الإخلال بسير نظام المعالجة عن قصد فهذه الجريمة من الجرائم العمدية التي تتطلب لقيامها توفر القصد الجنائي.

لذلك ندعو المشرع الجزائري أن يضيف مادة أخرى يكون نصها كالآتي..." يعاقب على الأفعال التي تعوق أو تعطل سير نظام المعالجة الآلية للمعطيات أو البيانات بالحبس من سنة إلى ٥ سنوات والغرامة من ٢٠٠,٠٠٠ إلى ١٠٠٠,٠٠٠ دج "...، خاصة وأنه صادق على الاتفاقية العربية سالفة الذكر.

الفرع الرابع : الجرائم الماسة بالمعلومات الشخصية وحاجة التشريع الجزائري لها

هناك العديد من الجرائم الماسة بالمعلومات الشخصية المتداولة في البيئة الإلكترونية نص عليها المشرع الفرنسي في التعديل الجديد لقانون العقوبات الفرنسي في الفصل الخامس المتعلق بحماية الحقوق الشخصية في المواد ٢٢٦/١٦،٢٢٦/٢٤، ٢٢٦/٣١ وهذه الجرائم هي:

-جريمة عدم الاتخاذ الإجراءات الأولية لإجراء معالجة البيانات.

-جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة.

-جريمة المعالجة غير المشروعة للبيانات.

-جريمة تسجيل وحفظ بيانات شخصية أو تتعلق بالماضي لأشخاص مصنفين.

-جريمة حفظ شخصية خارج الوقت المخصص به وفقا للطالب.

-جريمة تغيير الغرض المحدد لجمع البيانات الاسمية.

- جريمة إفشاء بيانات إسمية إضرار بصاحب الشأن.

المطلب الثاني: تجريم المساس بالمعلومات

المشرع هنا لا يحمي نظام البيانات من الناحية المادية أي البرامج والتطبيقات، إنما يسعى لحماية المعلومات الموجودة داخله لذلك يطلق البعض على هذه الجريمة **بالقرصنة المعلوماتية**.

الفرع الأول: جريمة التلاعب بالمعطيات داخل نظام المعالجة

نص المشرع على هذه الجريمة في المادة ٣٩٤ مكررا من قانون العقوبات حيث جاء فيها "يعاقب بالحبس من ٦ أشهر إلى ثلاث سنوات وبغرامة من ٥٠٠,٠٠٠دج إلى ٢٠٠٠,٠٠٠دج كل من أدخل بطريق الغش معطيات في نظام المعالجة

1- وهي كل الأعمال التى من شأنها منع النظام بصفة كلية أو جزئية عن العمل وقد ترد الإعاقة على برنامج من برامج التي يحتويها النظام... بالرجوع إلى التقرير التفسيري المتعلق بشرح اتفاقية بودابست للإجرام المعلوماتي نجد أنها تشترط أن تكون العرقلة على درجة من الخطورة بحيث يُحرم صاحب النظام من الاستعمال العادي لنظامه، ويدخل في ذلك منع الخدمة أو التشفير بسوء نية، غير أن النص الجنائي في القانون الفرنسي السالف الذكر لم يفرق... وبالتالي يستوي أن تكون الإعاقة دائمة أو مؤقتة أو على فترات، فتوقف بسيط في نظام المعالجة الآلية قد يحدث خللا يتسبب في خسائر فادحة.... أنظر، شيماء عبد الغني محمد عطالله، المرجع السابق، ص١٢٨.

2- وهو كل الأعمال التي تمس بحسن سير نظام المعالجة بحيث يجعل النظام غير قادر على أداء مهامه بصفة عادية، كالتقليل من سرعته أو عدم إتمامه للمهمة التي برمجَ لأجلها أو حتى الزيادة في سرعته بشكل يخل بالعمل به أنظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام التجارة الالكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤، ص٤١.

الآليـة أو أزال أو عـدل بطريـق الغـش المعطيـات التـي يتضمنها".

وجدير بالذكر أن هذه الأفعال تتعلق بالمعطيات في نظام المعالجة أي البيانات التي أدخلت إلى النظام من أجل معالجتها وتحولت إلى رموز وإشارات تجسد المعلومة، وعليه فإن هذه الجريمة لا تتعلق بالمعلومة في حد ذاتها، ولا تكون محلا لهذا السلوك المجرم المعلومات التى تم تحميلها على قرص مدمج لأنها إما أصبحت خارج النظام أو لم تتم معالجتها بعد، وعلى هذا الأساس فإن النص الجنائي هنا يحمي المعلومة المعالجة داخل النظام أو تلك التي مازالت في إطار المعالجة[1]... وبالرجوع إلى نص المادة السالف الذكر نجد أن السلوك المجرم يتحقق بـ:

– إدخال معطيات في نظام المعالجة: ويتحقق الإدخال عن طريق إضافة معطيات جديدة في نظام المعالجة الآلية[2]، الأمر الذي يؤثر على صحة البيانات الموجودة أو نسبتها أو قيمتها، وهذا النوع من السلوك يحدث عادة بمعرفة المسؤول عن القسم المعلوماتي المكلف بوظيفة المحاسبة والمعاملات المالية أو القائمين على المواقع الالكترونية، لذلك ترتبط هذه الجريمة غالباً بالمصارف والبنوك حيث يمكن لأي شخص يشغل مركز على قدر من الأهمية ولديه كفاءة فنية أن يتلاعب بالمعلومات الموجودة في الحاسب الآلي الخاص بهذه المؤسسات[3].

لكن هل يشترط أن يترتب على فعل إدخال معلومات على معطيات نظام المعالجة في ضرر أو تغيير لهذه المعطيات؟... المشرع لم يشر إلى وجوب وقوع ضرر أو حتى بقصد وقوع ضرر أو تغيير، وبالتالي فإن مجرد إدخال معلومات على معطيات نظام المعالجة يشكل السلوك المجرم لهذه الجريمة، كما لا يهم صحة المعلومات المدخلة من عدمه فالعبرة بالإدخال لا بمدى صحة هذه المعلومات.

– إزالة معطيات من نظام المعالجة: يقصد بالإزالة محو جزء أو كل المعطيات الموجودة داخل النظام أو تحطيم هذا النظام أو الدعامة الموجود بداخلها المعطيات، وكل ذلك يتم عن طريق برامج لها القدرة على محو هذه المعطيات[4].

– تعديل معطيات داخل نظام المعالجة: يقصد بالتعديل تغيير المعطيات الموجودة داخل النظام وتحريفها أو استبدالها بمعطيات أخرى[5]، ومن التطبيقات الشهيرة لفعل التعديل الواقع على المعطيات داخل نظام المعالجة قيام المتهم باقتطاع جزء بسيط من الحسابات الجارية في المؤسسة المالية التى يعمل لديها لتذهب إلى حسابه الخاص، وفي كل عملية يكون الفارق غير واضح بالنسبة للعملاء نظرا لضآلة قيمة الجزء المقتطع، لكنه يدر مالاً كثيراً على المدى الطويل بالنسبة للمتهم[6].

وتعتبر هذه الجريمة من الجرائم العمدية التي لا تقوم إلا بتوافر القصد الجنائي من علم وإرادة، والملاحظ أن المشرع أورد مصطلح "...بطريق الغش " أي أن هذه الأفعال يجب أن تتم بطريق الغش، وبالتالي يجب توفر سوء النية لدى الجاني عند إدخاله لمعطيات جديدة أو محو أو تغيير هذه المعطيات... لأن ذلك قد يتم برضا صاحبها وعلمه أو عن طريق الخطأ وهنا تنتفي المسؤولية، وتطبيقا لذلك قضي في فرنسا ببراءة المتهم الذي باع مجلة ملحقة بشريط ممغنط يحمل فيروس مما أدى إلى تدمير جميع المعطيات في النظام التابع للمشتري، لكن محكمة الاستئناف استندت في قرار التبرئة على أساس أن المتهم

1- لذلك يرى البعض أن الحماية الجنائية بخصوص هذه الجريمة تظل مستمرة طالما أن المعلومة داخل النظام في طريقها إلى المعالجة.. ينظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام... المرجع السابق، ص٤٥.

2- يصنف الفقهاء هذا النوع من السلوك ضمن الغش المعلوماتي الذي يتم عن طريق التلاعب وإدخال بيانات جديدة مصطنعة بغرض تغيير الحقيقة... ينظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام... المرجع السابق، ص٤٦.
ويتحقق هذا السلوك أيضا في الحالة التي يستخدم فيها حامل بطاقة الائتمان بطاقته ليسحب بها مبلغا أكبر من المبلغ المسموح به، وفي كل حالة تتم فيها الاستخدام التعسفي لبطاقة الائتمان لأنه يتلاعب بمعطياتها في كل حالة، ومن بين التطبيقات أيضا لجريمة إدخال المعلومات إلى المعطيات الموجودة داخل نظام المعالجة القيام بتدوين أسماء مستخدمين وعمال وهميين أو إبقائه على مستخدمين تم الاستغناء عنهم وتركوا الوظيفة، وبدل من أن يحفظ ملفاتهم أو يتعاقد معهم كما في الحالة الأولى فإنه يبقى كل ذلك صوريا ويستفيد هو من رواتبهم و امتيازاتهم

3- وكمثال على ذلك ما قامت به مستخدم يعمل لدى فرع مصرفي حيث اختلس ما يقارب ٧ مليون فرنك فرنسي... وذلك عن طريق تحويل لنقود وهمية مستخدما في ذلك الحاسب الآلي الخاص بهذا الفرع ثم قام بنقلها بواسطة محررات مصطنعة إلى حسابه الخاص بعد أن كان تلاعب في معطيات الذاكرة الخاصة بالحاسب الآلي... ينظر، عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام... المرجع السابق، ص٤٧.

4- أنظر، شول بن شهرة، المرجع السابق، ص١٠٢... أنظر أيضا.. خثير مسعود، الحماية الجنائية لبرامج الحاسب الآلي، مذكرة ماجستير، كلية الحقوق، جامعة أبي بكر بلقايد تلمسان، ٢٠٠٨، ص١٠٢.
وقد ورد في التقرير التفسيري لاتفاقية بودابست للإجرام المعلوماتي أن الإتلاف أو المسح أو الإلغاء هي جميعها أعمال تتعلق بالتلاعب في الأجهزة وتضر بعملية التسجيل والمد بالبيانات والبرامج.

5- وتطبيقا لذلك قضي في فرنسا بتوافر هذه الجريمة في حق المتهم الذي قام بتعديل الفيشات الورقية الخاصة بالشركة التي تعمل بها ثم قامت بإدخالها في جهاز الكمبيوتر بالشركة... أنظر، شيماء عبد الغني محمد عطالله، المرجع السابق، ص١٣٥.

6- ومن التطبيقات العملية لهذا السلوك قيام أحد المجرمين في ألمانيا بزرع فيروس في شبكة المعلومات متعلق بمستخدمي نظام خاص وذلك من أجل جمع معلومات شخصية لمستعملي هذا النظام بالإضافة إلى تعديل بعض البيانات المتعلق بهم. أنظر، رامي حليم، المرجع السابق، ص١٧.

لم يكن يعلم بوجود فيروس داخل القرص المرفق أي عدم توفر نية الغش لديه[1].

وعليه يجب في هذه الجريمة أن تتجه إرادة الجاني إلى فعل الإدخال أو الإزالة أو التعديل ثم يعلم أن نشاطه غير مشروع وأنه يعتدي على صاحب الحق في المعطيات ومع ذلك تتجه إرادته إلى ارتكاب الفعل، وفي هذه الحالة يتوفر القصد الجنائي[2].. وترى محكمة النقض الفرنسي أن نية الغش يمكن استخلاصها من واقعة الإدخال مثلا فاستعمال قنبلة معلوماتية أو فيروس يدل على نية الغش لدى المتهم[3].

من خلال العرض السابق لجريمة المساس بالمعطيات داخل نظام المعالجة نلاحظ أن المشرع قد نص على معظم الأفعال التي يمكن أن تمثل الركن المادي لهذه الجريمة، ومن جهة أخرى أكد على عمدية هذه الجريمة من خلال تكراره لمصطلح بطريق الغش في نص المادة السالف الذكر.. لكن الملاحظ أن العقوبة ليست على قدر خطورة الجريمة التي يمكن أن تنجر عنها خسائر باهظة خاصة في مجال المعاملات التجارية الإلكترونية التي تتم ما بين الشركات والمؤسسات، لذلك يكون من الضروري ترقية هذه الجريمة إلى مصاف الجنايات لتكون المادة ٣٩٤ مكررا من قانون العقوبات نص على النحو الآتي.."يعاقب **بالسجن من ٥ سنوات إلى ١٠ سنوات وبغرامة من ١٠٠٠,٠٠٠ دج إلى ٧٠٠٠,٠٠٠ دج** كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

الفرع الثاني : تجريم التصرف في المعطيات بصفة غير شرعية

نص المشرع على هذه الجريمة في المادة ٣٩٤ مكرر٢ من قانون العقوبات حيث جاء فيها "يعاقب بالحبس من شهرين إلى ثلاث سنوات و بغرامة مالية من ١٠٠٠,٠٠٠دج إلى ٥,٠٠٠,٠٠٠دج كل من يقوم عمداً و عن طريق الغش بما يأتي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الإنجاز في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

وهو ما نصت عليه الاتفاقية العربية لمكافحة الجريمة المعلوماتية في نص المادة ٠٩ منها [4]..

والهدف من تجريم هذه الأفعال هو حماية المعطيات خارج نظام المعالجة فلا يشترط في هذه الجريمة أن تكون المعطيات داخل نظام المعالجة، فالحماية هنا تشمل المعطيات في أي موضوع كانت سواء على أقراص ممغنطة أو مرسلة على طريق منظومة معلوماتية.

ومن خلال نص المادة٣٩٤ مكرر٢ السالف الذكر نجد أن الركن المادي لهذه الجريمة يضم السلوكات التالية :

–التصرف في معطيات لها علاقة بالجرائم الماسة بنظام المعالجة الآلية للمعطيات: ويكون ذلك إما عن طريق **تصميم معطيات** لهذا الغرض كإعداد الفيروسات أو القنابل الإلكترونية أو مواقع وهمية[5].

ومن بين الطرق التى ذكرتها المادة أيضا نجد **البحث** ويقصد المشرع هنا البحث في كيفية تصميم هذه المعطيات أو إجراء بحوث لتطويرها وإن كانت العبارة جاءت عامة[6]... وذكر النص بعد البحث مصطلح **التجميع**.. ويعني قيام الجاني بجمع عدد من المعطيات التي يمكن

1- أنظر، شيماء عبد الغني محمد عطاالله، المرجع السابق، ص١٣٨.

2- أنظر، مدحت رمضان عبد الحليم، المرجع السابق، ص٥٩-٦١.

3- أنظر، شيماء عبد الغني محمد، المرجع السابق، ص١٣٨... أنظر أيضا، خثير مسعود، المرجع السابق، ص٩٩.

4- حيث جرمت هذه المادة :

١ – إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ- أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب- كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

٢- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه s بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

5 – ينظر، حكم محكمة عنابة رقم ٠٥٦٣٧/١٠ الصادر بتاريخ ٢٠١٠/٠٦/٢٨ ، حيث جاء في منطوق الحكم " ... وأن الطريقة المستعملة لتحويل الاموال تتمثل في إنشاء مواقع شبيهة بالمواقع الرسمية لبعض البنوك، وعند محاولة الزبائن إجراء عمليات مصرفية بحساباتهم البنكية يجدون أنفسهم بالمواقع الخاطئة، التي أنشأها القراصنة دون علم فيقدمون لهم الأرقام الحسابية والارقام السرية التي تستعمل فيما بعد لتحويل الأموال.." .

كما أشارت محكمة باتنة في حكمها السالف الذكر إلى سلوك التصميم حيث جاء فيه " .. حيث أن المتهم أكد أنه يعمل بطريقة غير شرعية في مجال تصميم مواقع الأنترنيت ..." .

6- وقد تساءل الكثير عن من يشغل أحد محركات البحث للبحث عن مواقع متخصصة في تعليم كيفية الاختراق هل يعد مرتكبا لهذه الجريمة ؟ أم أن البحث أضيق من هذا المقصود ؟، لكن التوسع في مصطلح البحث من شأنه أن يوسع من نطاق الجريمة.

أن ترتكب بها الجريمة مما يشكل خطراً وهو ما جعل المشرع يتدخل لتجريم هذا الفعل[1].

كما نجد من بين الأفعال المجرمة أيضا فعل **التوفير**[2]، ومفاد ذلك تقديم المعطيات وإتاحتها لمن يريدها وجعلها في متناول الجميع[3]...، وإلى جانب فعل التوفير نجد **النشر** ويتمثل في إذاعة المعطيات محل الجريمة، ويعتبر هذا السلوك خطيراً جداً كونه ينقل المعطيات إلى عدد كبير من الأشخاص مما يزيد في احتمال وقوع الجريمة[4]، كما جرمت المادة السالفة الذكر فعل **الإتجار** بمعطيات لها علاقة بالجرائم الماسة بنظام المعالجة الآلية للمعطيات[5]، ويتم ذلك عن طريق تقديمها للغير بمقابل[6].

ويشترط للعقاب على هذه الأفعال أن تقع على معطيات مخزنة داخل أقراص أو ما شابه أو معالجة في نظام للمعالجة أو مرسلة عن طريق إحدى المنظومات المعلوماتية، مع إمكانية أن ترتكب بهذه المعطيات جرائم تمس نظام المعالجة، فإذا كان من غير الممكن أن ترتكب بها هذه الجرائم فلا تقوم الجريمة.

– التصرف غير المشروع في المعطيات المتحصل عليها من الجرائم الماسة بنظام المعالجة الآلية للمعطيات: وهي الصور الثانية لجريمة التصرف في المعطيات بصفة غير شرعية.. الواردة في نص المادة ٣٩٤ مكرر٢ السالفة الذكر، وتتحقق هذه الجريمة عن طريق **حيازة هذه المعطيات كالاحتفاظ بها أو تحميلها على** جهاز الحاسب الآلي الخاص بالمتهم، ومن بين سلوكيات المجرم أيضا نجد **الإفشاء أو النشر** ويفترض هذا السلوك خروج المعطيات المحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة من حيازة الجاني إلى الغير، ويحاول المشرع من خلال هذا السلوك تضيق دائرة الحائزين على هذه المعطيات، والملاحظ أن الإفشاء أو النشر يتم عادة بدون مقابل مع أن السلوك الأكثر وقوعاً هو الاتجار بهذه المعطيات وهو مالم ينص عليه المشرع، ويتوجب على القضاء في هذه الحالة إعتبار الإتجار من قبيل الإفشاء بمقابل حتى لا يفلت الجاني، وهو ما قضي به مجلس قضاء باتنة في القضية السالفة الذكر[7]، كما يعاقب المشرع على نشر المعطيات المتحصلة من هذه الجرائم[8]، ولا تهم الجهة التى تم الإفشاء لها، ولعل هذا السلوك يتعلق بالأشخاص الذين يمكنهم الحصول على مثل هذه المعطيات بسبب الوظيفة التى يشغلونها، وقد تقع من غير المجرم الذي أقدم على المساس بنظام المعالجة.. كأن تكون هذه المعطيات انتقلت إليه بطريقة ما وقام هو بإفشائها أو نشرها، ولا تهم الوسيلة التى يتم بها النشر سواء كانت تقليدية أو إلكترونية بل إن المشرع توسع ليشمل التجريم الاستعمال لأي غرض كان.

قد يقوم الجاني باستعمال هذه المعطيات، ويشمل التجريم كل استعمال للمعطيات السالفة الذكر مهما كان الهدف منها، ومثال ذلك قيام شركة ما باستعمال معلومات أو معطيات متحصل عليها بطريقة غير شرعية بإحدى الجرائم المذكورة آنفا تتعلق بشركة منافسة للإضرار بها[9] .

وتعتبر هذه الجريمة من الجرائم العمدية التي يتطلب قيامها إثبات القصد الجنائي بعنصريه العلم والإرادة لدى المتهم، وذلك بأن يعلم أنه يصمم أو يبحث أو يجمع أو يوفر أو ينشر.. في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية...، وأنّ هذه المعطيات يمكن أن تكون وسيلة لارتكاب الجرائم الماسة بنظام المعالجة الآلية للمعطيات...، وأن يقوم بهذه الأعمال

---

1 – لقد قدر المشرع أن تجميع عدد من المعطيات المستعملة لارتكاب هذا النوع من الجرائم من شأنه أن يرفع درجة الخطر التي تشكلها، مما يؤدي إلى إمكانية ارتكاب هذه الجرائم بل ويسهل ارتكابها...، أنظر، محمد خليفة، المرجع السابق، ص ٢٣٤.

2 – ويكمن الفرق ما بين التجميع والتوفير في أن التجميع لا يعدو أن يكون حيازة للمعطيات بينما يقضي التوفير وضع هذه المعطيات تحت تصرف أشخاص آخرين...، أنظر، محمد خليفة، المرجع السابق، ص ٢٣٦.

3– وقد تعرضت محكمة باتنة لهذا السلوك في منطوق حكمها حيث جاء فيه ".. حيث أن نشر المعطيات الألية المتحصل عليها من قبل المتهم والخاصة بمختلف الشركات ...ثابت في حقه باعترافه بإرساله تلك المعطيات إلى أحد القراصنة ووعده بعدم نشر صورة الشركة الامريكية..". أنظر، حكم محكمة باتنة رقم ١٠/٠٥٢٧٢ الصادر بتاريخ ١٠– ٠٦– ٢٠١٠.

4– ولم ينص المشرع الفرنسي على هذا الفعل في حين نصت عليه اتفاقية بودابيست في مادتها السادسة وجاء في التقرير التفسيري لها أن مصطلح النشر diffusion ينبغي ان يمتد ليشمل كل نشاط من شأنه نقل البيانات للغير..ينظر، هلالي عبد الإله أحمد، المرجع السابق، ص ٨١.

5 – لم ينص المشرع الفرنسي على هذا الفعل في المادة ٣٢٣-٣-١ من قانون العقوبات بينما تضمنت اتفاقية بودابيست مصطلحي البيع والاستيراد.

6 – وهو ما استند عليه حكم محكمة عنابة في قضية إنشاء مواقع وهمية حيث جاء فيه" وكشفت التحريات أن المسمي ...تلقي ثلاثة تحويلات مالية من كندا خلال سنتي ٢٠٠٧ – ٢٠٠٩أرسلتإليه من طرف الأشخاص الذين باع لهم موقع البنك الكندي الوهمي الذي قام بإنشائه هو لتضليل زبائن البنك.." وهنا يكمن الفرق ما بين فعل الإتجار وفعل التوفير الذي يكون عادة بدون مقابل. أنظر، حكم محكمة عنابة رقم ١٠/٠٥٦٣٧ الصادر بتاريخ ٢٠١٠/٠٦/٢٨.

7 – حيث جاء في منطوق القرار" ...حيث أنه ثبت للمجلس أن المتهم قد تاجر في المعطيات التى تحصل عليها بواسطة القرصنة والاختراق غير المشروع وهذا ما تؤكده الحوالات المالية التي تحصل عليها المتهم عن طريق وسترن يونين.. " أنظر، خليفة محمد، المرجع السابق، ص ٢٤٧.

8– وهو ما قضي به حكم محكمة باتنة في القضية السالفة الذكر حيث جاء فيه "..كما تأكد للجهات المختصة بمكافحة الجريمة المعلوماتية من خلال قراءة وتتبع نشاط المتهم أنه قام بنشر كل المعطيات عبر شبكة الأنترنيت مع وضع صورة للمؤسسة المخترقة.."

9 – ومن هنا يتوجب على من يحصل على مثل هذه المعطيات ألا يحتفظ بها أو يتصرف فيها لأنها تعتبر عائدات إجرامية، وهذا شرط أساسي في هذه الجريمة فإذا لم تكن هذه المعطيات متحصل عليها من الجرائم الماسة بنظام المعالجة الآلية للمعطيات فلا يقوم هذا السلوك المجرم.

بإرادته الكاملة[1]، ويتحقق القصد الجنائي في الصورة الثانية للجريمة عندما يكون الجاني عالماً بأنه يحوز أو ينشر أو يستعمل معطيات متحصل عليها من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، ولا يهم الغرض من هذه الأفعال فالأهم هو أن هذه المعطيات متحصل عليها من الجرائم السابقة الذكر ثم يجب أن يقوم بهذه الأفعال بحريمة وإرادة تامة وعندها يتحقق القصد الجنائي بعنصريه.

والملاحظ أنّ المشرّع لم يتوقف عند اشتراط توفر العمد في هذه الجريمة لكنه اشترط أيضا توافر الغش لدى المتهم أي يجب أن تتوفر نية الاحتيال والتدليس لدى الجاني وهو أمر يمكن أن يستخلص من وقائع الحال...، **ومع ذلك نجد أنه من الأفضل الاستغناء عن هذه العبارة والاكتفاء بعبارة " عمدا "، حتى لا يفلت المجرمون من العقاب بداعي عدم توافر حالة الغش.**

لقد جرم المشرع التصرف غير المشروع في المعطيات سواء كان ذلك للحيلولة دون وقع الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، أو منعاً للتصرف في المعطيات المتحصلة منها، وقد أسهب المشرع في سرد الأفعال التي يمكن تشكل هذا الفعل المجرم، ومع ذلك لم تكن العقوبة كافية بالنظر لخطورة الأفعال لذلك نقترح أن يكون نص المادة ٣٩٤ مكرر٢ من قانون العقوبات على النحو التالي: **"يعاقب بالحبس من ٦ أشهر إلى خمس سنوات وبغرامة مالية من ١،٠٠٠،٠٠٠دج إلى ٥،٠٠٠،٠٠٠ دج كل من يقوم عمداً بما يأتي:**

– تصميم أو بحث أو تجميع أو وضع تحت التصرف أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو الإتجار أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

المبحث الثاني : المكافحة الإجرائية للجريمة المعلوماتية

تتضمنُ المكافحة الإجرائية إجراءات البحث والتحري وجمع الاستدلالات والتحقيق والتي تهدف إلى الكشف عن الجريمة، والأمر لا يثير الكثير من الصعوبات إذا وقع التحقيق والبحث على حواسيب وأجهزة تقنية وأقراص... وغيرها من الأجهزة ذات الطابع المادي[2]، الإشكال يثار بشأن معاينة العلم الافتراضي أين تقل فرص العثور على الأدلة والتوصل إلى مجرمين، لذلك يكون من الضروري اللجوء إلى بعض الأساليب الإلكترونية والقانونية والتي تساعد في الوصول إلى الحقيقة.

ويعتبر المشرع الجزائري رائدا في هذا المجال– من الناحية التشريعية على الاقل– وذلك بإصداره للقانون رقم ٠٤/٠٩ المتعلق بمكافحة جرائم تكنولوجيا الإعلام والاتصال والوقاية منها[3]...، وكذا مصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وسنتناول هذا القانون بشيء من التفصيل للوقوف على أهم ما جاء فيه.

المطلب الأول : التسرّب " نظام المرشد الجنائي "

عجز الأجهزة المختصة عن البحث والتحقيق في الجرائم الإلكترونية، دفع بالكثير من التشريعات لاستحداث أساليب تسمح بالتواجد في مسرح الجريمة وضبط المجرمين في حالة تلبس وهو ما يعرف بنظام الإرشاد الجنائي[4] .

ويعتبر نظام الإرشاد الجنائي ذا أهمية كبيرة في مثل هذه الجرائم التى يصعب الكشف عنها، إذ من شأنه أن

---

1 – وقد جاء في حكم محكمة باتنة السالف الذكر إشارة إلى عنصر العلم بقولها " ..من خلال قيام المتهم بارتكاب الأفعال المتابع بها من خلال قيامه بإنشاء موقع مشابه للموقع الخاص بالبنك الكندي، مع علمه مع علمه أن الموقع يخص طرفا لا علاقة له به .. مما جعل الركن المعنوي متوفرا في حقه..".
ولكن هل يشترط أن يكون لدى الجاني نية استعمال هذه المعطيات في إحدى الجرائم الماسة بأنظمة المعالجة الآلية ؟ وبعابرة أخرى هل يتوجب توفر قصد جنائي خاص في هذه الجريمة ؟... لابد من الاعتراف بأنه لا يمكن مساءلة أي شخص يقوم بالتعامل في هذه المعطيات إلا إذا كان له قاصداً استعمالها في الجرائم المذكورة آنفا، وهو يمكن القول معه أنه لابد من توافر قصد خاص في هذه الجريمة وهو نية استعمال هذه المعطيات في ارتكاب إحدى الجرائم الماسة بأنظمة المعالجة، وهو ما أشارت إليه اتفاقية بودابيست في مادتها السادسة عندما اشترطت صراحة وجوب توفر هذا مثل هذا القصد.

2– إذا اتضح للجهات القائمة على البحث والتحري أنه يمكن القيام بمعاينة مسرح الجريمة فيتوجب عندها مراعاة عدة قواعد وإرشادات فنية أهمها:
- تصوير الحاسب الآلي والأجهزة المتصلة به.
- معاينة واثبات حالة التوصيلات والكابلات المتصلة لكل مكونات النظام.
- عدم نقل أية مادة معلوماتية قبل إجراء اختبارات عليها من طرف اختصاصي لكيلا يؤدي ذلك إلى إتلافها.
– التحفظ على محتويات سلة المهملات وكذا مستندات الإدخال والإخراج الورقية المتعلقة بالحاسب .

3– القانون رقم ٠٤/٠٩ الصادر بتاريخ ٥ أوت ٢٠٠٩ ج ع ٤٧.

4– وهو ما تضمنته التوصية التى أقرها المجلس الاوربي الخاصة بالمشاكل الإجرائية المتعلقة بتكنولوجيا المعلومات سنة ١٩٩٥...ينظر، شول بن شهرة، المرجع السابق، ص ٢٢٥ .

يحاصر النشاط الإجرامي، ويقلص الفوارق الموجودة بين مرتكب الجريمة ومكان البحث عنها... وتقتضي هذه التقنية أن يدخل أحد رجال الضبطية أو أحد أعوانها[1] إلى بيئة الأعمال الإلكترونية، والدخول في نقاشات مع الغير عن طريق استخدام أسماء مستعارة إذا تبين لهم وجود نية إجرامية مع الأشخاص الذين يتواصلون معهم، وعندها يحاولون التعرف على هوياتهم الحقيقية حتى يتمكنوا من القبض عليهم....، وكمثال على ذلك ما قامت به المباحث الفدرالية الأمريكية عندما دست أحد أعضائها لكي يتمكن بعد ذلك من ضبط مجموعة من المجرمين تمتهن قرصنة البرمجيات والمتاجرة فيها بطريقة غير مشروعة[2].

تقتضي هذه التقنية أن يدخل أحد رجال الضبطية أو أحد أعوانها إلى البيئة الإلكترونية، ثم الدخول في نقاشات مع الغير عن طريق استخدام أسماء مستعارة إذا تبين لهم وجود نية إجرامية مع الأشخاص الذين يتواصلون معهم، وعندها يحاولون التعرف على هوياتهم الحقيقية حتى يتمكنوا من القبض عليهم[3]....، وبالرجوع إلى المشرع الجزائري لا نجد مثيل لهذا النظام في القانون رقم ٠٤/٠٩ المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها، غير أنه قد نظم عمل المرشد الجنائي تحت مصطلح التسرب، حيث جاء في المادة ٦٥ مكرر ١٢ من قانون الإجراءات الجزائية أنه يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جنحة أو جنائية بإيهامهم أنه فاعل معهم أو شريك....، كما نصت المادة ٦٥ مكررا١ من قانون الإجراءات الجزائية على أنه يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن بمباشرة عملية التسرب ضمن الشروط القانونية... وقد سمح المشرع للضابط المتسرب أن يستعمل هوية مستعارة وأن يجوز أو ينقل أو يسلم أو يعطي مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، كما يسمح له وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي.. أو الاتصال[4].

وحسب المادة ٦٥ مكرر١٥ لا يمكن القيام بهذا الإجراء من قبل ضابط الشرطة وأعوانهم إلا بإذن من وكيل الجمهورية أو قاضي التحقيق، والذي يشترط أن يكون مكتوباً ومسبباً تحت طائلة البطلان... حيث يذكر فيه الجريمة المراد التسرب فيها وهوية ضابط الشرطة أو العون الذي تتم العملية تحت مسؤوليته، علما أن مدة التسرب لا يمكن أن تتجاوز ٤ أشهر إلا إذا وجدت ضرورة لمقتضيات التحري أو التحقيق، ويجوز للقاضي الذي رخص بإجرائه بأن يأمر في أي وقت بوقفه قبل انقضاء هذه المدة.

وإذا تقرر وقف عملية التسرب وفي حالة عدم تمديدها يمكن للعون المتسرب مواصلة نشاطاته للوقت الضروري الكافي لتوقيف المراقبة في ظروف تضمن أمنة، دون أن يكون مسؤولاً جزائياً.. على ألا يتجاوز ذلك مدة ٤ أشهر٥.

المطلب الثاني: التفتيش في البيئة الإلكترونية

التفتيش إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة الجريمة، وبما أن التفتيش يمس بحرية الإنسان وحرمة حياته الخاصة،فقد أحطتها التشريعات بإجراءات وشروط خاصة[6]، ويختلف التفتيش الإلكتروني عن التفتيش في الجرائم الأخرى، فالمحل بين الجريمتين مختلف، فهل تختلف الشروط والضمانات أيضا؟..

الفرع الأول : بين التفتيش العادي والإلكتروني

يشمل التفتيش في بيئة الأعمال الإلكترونية محلين، المحل الأول هو جهاز الحاسوب بمكوناته المادية

1- هذه الجرائم تتطلب اللجوء إلى أشخاص ذوي خبرة في الاتصالات والأنترنيت للقيام بهذه المهمة.. ينظر، نبيلة هبة هروالة، المرجع السابق، ص١٦٩.

2- ومن أمثلة ذلك أيضا دخول ضابط الشرطة أو العون المكلف بالإرشاد في محادثات مع أحد المراكز أو المشتبه فيهم الذي ينوي الحصول على بطاقات ائتمان بطريقة احتيالية، فيسأله المرشد عن كيفية قيامه بذلك أو يطلب منه مساعدته أو الشراء منه من أجل القبض عليه متلبس بالجريمة.. ينظر، نبيلة هبة هروالة، المرجع السابق، ص١٦٩.

3- وكمثال على ذلك ما قامت به المباحث الفدرالية الأمريكية عندما دست أحد أعضائها لكي يتمكن بعد ذلك من ضبط مجموعة من المجرمين تمتهن قرصنة البرمجيات والمتاجرة فيها بطريقة غير مشروعة.

4- تجدر الإشارة إلى أن إجراء عملية التسرب فيها مساس بخصوصية الأفراد لذلك سمح بها المشرع في بعض الجرائم حيث ذكرت المادة ٦٥ مكرر ١١ أنه يجوز اللجوء إلى التسرب في إحدى الجرائم المذكورة في المادة ٦٥ مكرر وبالرجوع إلى هذه المادة نجدها تذكر جرائم المخدرات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالصرف وجرائم الفساد، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

5- تجدر الإشارة إلى الاتفاقية العربية لمكافحة الجريمة المعلوماتية لم تنص على مثل هذا الإجراء.

6- فوفقا للمادة ٤٤ من قانون الإجراءات الجزائية فانه " لا يمكن القيام بتفتيش مساكن الأشخاص إلا بشروط منها:

- وجود إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق؛
- حضور صاحب المسكن أو من ينوب عنه؛
- التفتيش في الأوقات المحدد قانونا وهي من الخامسة صباحا إلى الثامنة مساءاً حسب المادة ٤٧ من القانون السابق.

والمعنوية، والمحل الثاني الشبكة العنكبوتية وما تتضمنه من مكونات كالمواقع والبريد الإلكتروني وغيرها[1].

وقد أجاز المشرع بموجب المادة ٥ من القانون ٠٤/٠٩، للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وكل منظومة معلوماتية...، ومنه يتضح أن عملية التفتيش تنصب على جهاز الكمبيوتر وجميع الأجهزة التابعة له وهي مكونات مادية يسهل تفتيشها، إنما الإشكال يثار بشأن تفتيش المكونات المعنوية كالبرامج وقواعد البيانات وكذا المواقع في الشبكة العنكبوتية والبريد الإلكتروني وغيره، فهي تتطلب مهارة عالية وسرعة لفك الشفرات والتعرف على الجناة.

وما يلاحظ من نص المادة ٥ السالف الذكر أن التفتيش يكون بصفة مباشرة عن طريق الانتقال إلى مسكن المتهم أو المكان الذي تتواجد فيه أجهزته وهنا يجب الالتزام بشروط التفتيش الواردة في قانون الإجراءات الجزائية سواء من حيث الإذن أو الميعاد أو الكيفية، وقد يكون التفتيش عن بعد كما أشارت المادة السالفة الذكر، ويقضي ذلك الدخول إلى المنظومة المعلوماتية دون إذن صاحبها والولوج إلى حاسوبه والتفتيش فيه وفي برامجه.

ولكن هل يجوز الدخول إلى الحسابات الشخصية من أجل التفتيش فيها مثل البريد الإلكتروني ومواقع التواصل الاجتماعي كالفيس بوك وغيرها ؟

بالرجوع إلى المادة المذكورة أعلاه نجد أن المشرع أجاز التفتيش داخل المنظومات المعلوماتية أو جزء منها، فما المقصود بالمنظومة المعلوماتية ؟... أجابت على ذلك المادة ٢ من القانون ٠٤/٠٩، حيث جاء فيها تعريف للمنظومة المعلوماتية على أنها " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم وأحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين"، ومن خلال هذا التعريف نجد أن المشرع تفطن إلى أمر مهم جدا هو ارتباط الحواسيب ببعضها البعض، وهو ما يشكل ترابط في الأنظمة المعلوماتية على حد تعبير التعريف السابق، إذ أنه من المعلوم أن شبكة الأنترنيت شبكة ممتدة بين أجهزة الحواسيب مرتبطة ببعضها في مكان واحد ويطلق عليه الشبكة المحلية أو موزعة ومرتبطة بواسطة خطوط الهاتف والأقمار الصناعية.

وبناءا على ما سبق يمكن القول أن التفتيش في بيئة الأعمال الإلكترونية يشمل محلين، المحل الأول هو جهاز الحاسوب بمكوناته المادية والمعنوية، والمحل الثاني الشبكة العنكبوتية وما تتضمنه من مكونات كالمواقع والبريد الإلكتروني وغيرها.

ولكن إذا سلمنا بإمكانية التفتيش في بيئة الأعمال الإلكترونية، فهل تنسحب شروط التفتيش العادية إلى مجال التفتيش الإلكتروني؟...، يرتبط التفتيش بثلاثة شروط مهمة جدا وهي الإذن، والمدة، وحضور صاحب محل التفتيش، فبالنسبة للإذن نجد أن المشرع قد فصل في المسألة بموجب المادة الأولى الفقرة الرابعة من قانون ٠٤/٠٩، السالف الذكر حيث جاء فيها "لا يجوز إجراء عمليات في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

وإذا كان قانون الإجراءات الجزائية يحظر التفتيش من الثامنة ليلا إلى الخامسة صباحا، نظرا لتعلق الأمر بتفتيش المساكن وهو مستقر الإنسان ومكمن أسراره وحياته الخاصة، فإن الأمر يختلف نوعاً ما عن التفتيش في بيئة الأعمال الالكترونية، ومع ذلك لم يشر المشرع إلى مسألة ميقات التفتيش في القانون ٠٤/٠٩، ولكنه أحال ذلك إلى قانون الإجراءات الجزائية وهو ما يفهم من نص المادة ٥ حيث جاء فيها "يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي حالات المنصوص عليها في المادة ٤ أعلاه الدخول بغرض التفتيش ..." وهو ما يفضي بالضرورة إلى وجوب احترام ميعاد التفتيش الوارد في قانون الإجراءات الجزائية .

أما فيما يخص حضور صاحب المحل الذي يجري فيه التفتيش والذي يعد من الشروط الشكلية المعروفة في مجال التفتيش العادي، فإن الولوج إلى المواقع الإلكترونية أو البريد الإلكتروني يتطلب نوعاً من السرعة والسرية حتى لا يتم التلاعب بالأدلة، ورغم هذه الصعوبات إلى أن

1- وللتفتيش في البيئة الإلكترونية يتوجب التفرقة ما بين ٣ فرضيات الأولى في حالة اتصال حاسب المتهم بحاسوب آخر أو نهاية طرفيه موجودة داخل الدولة، فلا خلاف بين التشريعات في امتداد التفتيش إلى سجلات البيانات المتواجدة في الأجهزة الأخرى، وقد اشترط المشرع في هذه الحالة ضرورة إبلاغ السلطة القضائية المختصة حسب نص المادة ٥ من قانون ٠٤/٠٩،. أما في الفرضية الثانية وهي في حالة اتصال جهاز حاسوب المتهم بحاسوب أو نهاية طرفيه موجودة خارج إقليم الدولة فهنا يتعلق الأمر بالسيادة ولابد من وجود اتفاق مسبق ما بين الدولتين، وهو ما نصت عليه المادة ٥ السالفة الذكر حيث اشترط المشرع القيام بالتفتيش بمساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل ، ينظر، زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى عين مليلة الجزائر، ٢٠١٢، ص ١٤٠.

البعض ينادي بضرورة حضور المتهم أثناء التفتيش فإذا تعذر حضوره ينوب عنه شاهدين كضمانة للمتهم.

هذا وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية والتي صادق علها المشرع الجزائري في سبتمبر ٢٠١٤ على مسألة تفتيش المنظومة المعلوماتية حيث جاء في ٢٦ منها "

- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش

أو الوصول إلى:

أ) تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها؛

ب) بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.

٢- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها، بما يتوافق مع الفقرة (١ - أ) إذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

الفرع الثاني: ضبط الأدلة أثناء التفتيش الإلكتروني

وضع اليد على الأدلة للوصول إلى الحقيقة هو الهدف من التفتيش، وإذا كانت البيانات والمعطيات المخزنة في ذاكرة الحاسوب أو تلك المثبتة على دعامة لا تشكل عائقا عند توقيع أو الحجز عليها، فأن الأمر بالصعوبة بما كان إذ تعلق الحجز بالمعطيات أو المعلومات نفسها.

وبدون الخوض في الجدال الفقهي حول إمكانية الحجز من عدمها نجد أن المشرع انحاز إلى الاتجاه القائل بإمكانية حجز المعلومات[1]، وعلى هذا الأساس إذا توصل المحققون أثناء إجراء التفتيش إلى وجود معطيات من شأنها المساهمة في الكشف عن الجريمة فعليهم حجزها وذلك عن طريق نسخها في دعامة مادية أو اي وعاء للبيانات كطبعها على الورق، كما يمكن للسلطة المختصة وضع اليد على البرنامج كاملاً وكذا أنظمة تشغيله.

ويوجب القانون على السلطة القائمة على التفتيش والحجز السهر على سلامة المعطيات، ويجوز لها عند الضرورة استعمال الوسائل التقنية قصد جعلها قابلة للاستعمال لأغراض التحقيق شرط ألا يؤدي ذلك إلى المساس بمضمون هذه المعطيات.

ونظراً لخصوصية التفتيش والضبط في مجال الجرائم الإلكترونية، فإن المشرع قد أجاز للجهة المكلفة بالتفتيش الاستعانة بذوي الخبرة من مقدمي خدمة الأنترنيت... وعند الانتهاء من عملية ضبط الموجودات أثناء التفتيش الإلكتروني في إحدى الجرائم المعلوماتية، فإنه يتوجب على القائم بعملية التفتيش والضبط وضع هذه الموجودات المعنوية في دعائم كما ذكرنا سابقاً، ولا يتم فتحها إلا بحضور صاحبها مصحوباً بمحاميه[2].

هذا وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية على مسالة ضبط المعلومات المخزنة حسب نص المادة ٢٧ التي جاء فيها أنه :

١- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقرة (١) من المادة السادسة والعشرين من هذه الاتفاقية.. هذه الإجراءات تشمل صلاحيات:

أ) ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات؛

ب) عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها؛

ج) الحفاظ على سلامة معلومات تقنية المعلومات المخزنة؛

د) إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها.

٢- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية

١- أنظر،هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر، ١٩٩٤، ص ٩٣ وما بعدها.

2- هذا وقد نصت اتفاقية بودابيست على تفتيش وضبط البيانات المعلوماتية المخزنة، حيث أوجبت على كل دولة طرف سنّ تشريعات تمنح بموجبها السلطات المختصة بالتحقيق صلاحية التفتيش أو الولوج لكل نظام معلوماتي أو لجزء منه وكذلك للبيانات المعلوماتية المخزنة فيه وعلى إقليمه؛ ولكل دعامة تخزين عليها بيانات معلوماتية، كما تمنحها أيضا صلاحية ضبط أو الوصول نظام معلوماتي أو جزء منه أو إلى دعامة تخزين، أو التحقق والتحفظ على نسخة من هذه البيانات، أو المحافظة على سلامة البيانات المخزنة، أو منع حذف هذه البيانات من النظام .

المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين ٢ و١ من المادة السادسة والعشرين من هذه الاتفاقية".

الفرع الثالث: الأمر بحفظ المعطيات أو تسليمها

يهدف التفتيش عموما إلى الوصول إلى الحقيقة عن طريق وضع اليد على الأدلة، غير أن ضبط الأشياء المادية كالمستندات والأوراق ووسائل ارتكاب الجريمة يعد أمراً يسيراً مقارنة بتوقيع الحجز على منظومة معلوماتية، فالبيانات والمعطيات المخزنة في ذاكرة الحاسوب أو تلك المثبتة على دعامة لا تشكل عائقا عند توقيع أو الحجز عليها، في حين أن الأمر بالصعوبة بما كان إذ تعلق الحجز بالمعطيات نفسها[1].

بالرجوع إلى المادة ١٠ من القانون ٠٤/٠٩ السالف الذكر نجدها تلزم مقدمي الخدمات بتقديم المساعدة اللازمة للسلطات المكلفة بالتحريات القضائية، وذلك لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات عند إجرائها، وبوضع المعطيات التي يتعين عليهم حفظها، وهذا الأمر لا يتعلق بكل المعطيات وإنما يلتزم مقدمو الخدمات بحفظ المعطيات التالية :

-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال؛

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة ؛

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال ؛

- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها ؛

- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها؛.

أما بالنسبة للنشاطات المتعلقة بالاتصالات الهاتفية فإنه يتوجب على مقدم هذه الخدمة بحفظ المعطيات التالية:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة ؛

-المعطيات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه[2].

وإلى جانب التزامات مقدمي الخدمات بحفظ البيانات والمعطيات يتوجب عليهم أيضاً تسليم البيانات التي تكون بحوزتهم للسلطات المختصة عند طلبها منهم وأشارت المادة ٥ من القانون ٠٤/٠٩ أنه يجوز لسلطة التفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية قصد مساعدتهم وتزويدهم بالمعلومات التي يطلبونها منهم[3].

المطلب الثالث: ضرورة التعاون الدولي لموجهة الجرائم المعلوماتية

الجرائم المعلوماتية جرائم عابرة للحدود تتسم بالعالمية نظرا لارتباط الكثير من صورها بالشبكة العنكبوتية، فأطراف التعاملات الإلكترونية غالباً ما تكون ذات طابع دولي، وهذا الأمر لا يحكمه قانون موحد ذو طابع دولي بل تنظمه تشريعات الدول الداخلية، وهو ما يخلق مشكلة الاختصاص القضائي في حالة وقوع نزاع أو جريمة،

1- وقد ثار جدل فقهي حول إمكانية توقيع الحجز على المعطيات وهي منفصلة عن دعامتها فيرى اتجاه من الفقه الفرنسي أن برامج الحاسوب تعد كيانا ماديا ملموسا فهي عبارة عن نبضات أو إشارات إلكترونية، في حين يذهب اتجاه آخر أن المعلومات والبرامج على حالتها الأصلية لا تقبل التملك ولا الحيازة..... وهو ما أخذ به التشريع الألماني حيث نصت المادة ٩٤ من قانون الإجراءات الجزائية أن البيانات المعالجة لا يسوغ ضبطها إلا بعد تحويلها إلى كيان مادي.. ينظر، هشام محمد فريد، المرجع السابق، ص ٩٣ وما بعدها.

2- وهو أكدت عليه اتفاقية بودابيست المتعلقة بالإجرام المعلوماتي من أنه يتوجب على الدول الأعضاء اتخاذ القواعد القانونية اللازمة لإلزام المتدخلين مثل مزودي الخدمات، من أجل المبادرة بحفظ البيانات المخزنة لديه في مرحلة أولى ثم الكشف عنها في مرحلة ثانية لسلطات البحث، مع ضرورة ضبط آجال الحفظ، والملاحظ أن الاتفاقية لم تبين الكيفية التي يتم بها هذا الحفظ، وبذلك أوكلت الأمر لكل دولة طرف عن طريق سن الإجراءات الضرورية للسماح لسلطاته المختصة أن تفرض أو تأمر بالتحفظ على البيانات المعلوماتية المخزنة بواسطة نظام معلوماتي، عندما تكون هناك أسباب تدعوا للاعتقاد بأن هذه البيانات معرضة للإتلاف أو التزوير أو للتغيير.

كما أشارت الاتفاقية إلى مسألة التحفظ والكشف أو الإفشاء العاجلان لبيانات المرور وأكدت أنه يتوجب على كل طرف اتخاذ جميع الإجراءات اللازمة للتحفظ على البيانات المتعلقة بالمرور لأجل:

- توفر التحفظ العاجل لهذه البيانات المتعلقة بالمرور بغض النظر عن وجود مزود خدمات واحد أو عدة مزودين ساهموا في نقل الاتصال.
- إبلاغ السلطة المختصة عن كمية بيانات كافية لتحديد هوية مزودي الخدمات وطريق الاتصال الذي جرى.

3- وهو ما أشارت إليه اتفاقية بودابيست من أنه يتوجب على كل دولة طرف أن يتخذ الإجراءات الضرورية التي تسمح لسلطاتها المختصة أن تأمر أي شخص يتواجد على إقليم تلك الدولة بإرسال بيانات في حوزته سواء كانت مخزنة في نظام معلوماتي أو على دعامات تخزين، وكذا مقدم الخدمات الذي يقدم خدماته على إقليمها من أجل إرسال البيانات التي في حوزته والمتعلقة بالمشتركين وبالخدمات التي يقدمها..؛ وكل ذلك في سبيل تحديد نوعية خدمة الاتصال وتقنياتها الفنية، أو تحديد الهوية، أو العنوان، أو رقم الهاتف، أو بيانات دفع الفاتورة والمبلغ المدفوع، أو أي بيانات أخرى متوافرة على أساس عقد أو اتفاق تقديم الخدمة .

الأمر الذي يجعل من التعاون الدولي في هذا المجال ضرورة حتمية سواء من حيث الوسائل أو التشريعات[1].

الجريمة المعلوماتية لا تعرف الحدود الجغرافية.. فهي جرائم عابرة للحدود، وهو ما يجعل من التعاون الدولي مطلب الجميع، لهذه الأسباب سارعت بعض الدول إلى النص على صور التعاون الدولي في مجال إجراءات المتابعة والتحقيق، وإبرام اتفاقيات دولية لتبسيط هذه الإجراءات وتوحيد القواعد العامة، وقد نصت اتفاقية بودابيست، على المبادئ العامة إلى تحكم التعاون الدولي في مجال الجرائم التي لها علاقة بالجرائم المعلوماتية.

هذا وقد حثت الاتفاقية العربية لمكافحة الجريمة المعلوماتية التي صادق عليه المشرع الجزائري على مسألة التعاون الدولي حيث جاء في المادة ٣٢ منها ما يلي :

١-على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى يمكن لغايات التحقيقات أو

الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم.

٢-تلتزم كل دولة طرف بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين

٣-يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطيويجوز لكل دولة طرف الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني على أنتضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير) وتأكيدالإرسال حسبما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبلوتستجيب للطلب بوسيلة عاجلة من الاتصالات.

٤- باستثناء ما يرد فيه نص في هذا الفصل فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة لمتبادلة بما في ذلك الأسس التي كان للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية.

٥-حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم فإن هذا الشرط يعتبر حاصلا بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف"[2].

الفرع الأول: المساعدات القضائية الدولية

المساعدة القضائية الدولية هي كل إجراء قضائي تقوم به الدولة في سبيل تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم الواقعة في بيئة الاعمال الالكترونية؛ وقد تنبه المشرع الجزائري إلى أهمية هذا الإجراء فسمح في إطار التحريات أو التحقيقات القضائية بخصوص الجرائم الواقعة في بيئة الأعمال الإلكترونية وبالتحديد تلك المتعلقة بأنظمة المعالجة الألية للمعطيات، والتي تعتبر من صور الجريمة المعلوماتية، سمح للسلطات المختصة بتبادل المساعدة القضائية الدولية بخصوص جمع الأدلة الإلكترونية، بل يمكن في حالة الاستعجال قبول طلبات المساعدة القضائية إذا وردت عن طريق وسائل الاتصال الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط تضمن أمنها

1- إن الجرائم محل الدراسة من الخطورة إلى درجة أن القواعد العامة تقف عاجزة عن التصدي لها كما رأينا سلفا، فالسلوك المجرم يقع في بلد وتحقيق نتيجته في بلد آخر أما المساهمون فهم في بلد ثالث وهكذا، لذلك لابد من وجود تعاون دولي سواء من الناحية الموضوعية أو من الناحية الإجرامية، ينظر في هذا المعنى .. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، ط١، الإسكندرية، ٢٠٠٨، ص ٣٩٣.

2- هذا وقد أشارت الاتفاقية العربية لمكافحة الجريمة المعلوماتية التي صادق عليه المشرع الجزائري على مسألة غاية في الأهمية تتعلق بالاختصاص الدولي حيث جاء في المادة ٣٠ منها "
١-تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجر يمة كليا أو جزئيا أو تحققت:
أ) في إقليم الدولة الطرف ؛
ب) على متن سفينة تحمل علم الدولة الطرف ؛
ج) على متن طائرة مسجلة تحت قوانين الدولة الطرف؛
د) من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان
ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة ؛
ه) إذا كانت الجريمة تمس أحد المصالح العليا للدولة.
٢-تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة ٣١ الفقرة (١) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.
٣-إذا ادعت أكثر من دولة طرف بالاختصاص القضائي الجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو صالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم ".

وصحته[1] ويمكن حصر المساعدات الدولية المتبادلة في الصور التالية :

أولا : تبادل المعلومات ونقل الإجراءات بين الدول

بالرجوع إلى المادة ١٧ من قانون ٠٩/٠٤ المتعلق بالوقاية من جرائم تكنولوجيا الاعلام الاتصال نجد أنه تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقاً للاتفاقية الدولية ذات الصلة والاتفاقيات الثنائية ومبدأ المعاملة بالمثل .

أما عن نقل الإجراءات فيتمعن طريق قيام دولة بإتخاذ إجراءات جنائية بمناسبة جريمة معينة قد أرتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة وذلك بناءا على اتفاقية مبرمة بينهم، وذلك بأن ترسل دولة لدولة أخرى معلومات حصلت عليها أثناء التحريات الخاصة بها، إذا رأت أن هذه المعلومات يمكن أن تساعد الدولة المرسل اليها في اجراء تحقيقات متعلقة بإحدى الجرائم الواردة في المعاهدة المبرمة بينهم[2].

وبالرجوع إلى الاتفاقية العربية السالفة الذكر نجدها تنص على مثل هذا الإجراء في نص المادة ٣٩ منها حيث جاء فيها "

١ – يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأم أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي حفظها بحسب المادة السابعة والثلاثين

٢–تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقا للأحكام الواردة في هذه الاتفاقية.

٣–تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل"[٣].

ثانيا : الإنابة القضائية على المستوى الدولي

نظم المشرع إجراءات الإنابة القضائية في المواد ٧٢١ و٧٢٢ من قانون الإجراءات الجزائية أن المشرع قد نظم، حيث جاء في المادة الأولى أنه في حالة المتابعات الجزائية غير السياسية في بلد أجنبي تسلم الإنابات القضائية الصادرة من السلطة الأجنبية بالطريق الدبلوماسي، وتنفيذ الإنابات القضائية وفقاً للقانون الجزائري ومبدأ المعاملة بالمثل.

وتتمالإنابة القضائية الدولية عند طلب إحدى الدول من دولة أخرى اتخاذ إجراء من إجراءات الدعوى الجزائية للفصل في مسألة معروضة على السلطة القضائية لدى الدولة صاحبة الطلب، وكمثال على ذلك طلب دولة ما إجراء التفتيش أو الضبط والمعاينة في دولة أخرى، وتتم هذه الإجراءات وغيرها عن طريق إرسال ملف الدعوى ومحاضر الاستدلالات عبر القنوات الدبلوماسية بوزارة الخارجية ثم سفارة الدولة متلقية الطلب.

ثالثا : تسليم المجرمين

الجرائم المعلوماتية تهدد استقرار التعاملات الإلكترونية وأمن المعلومات، لذا يعد الاتفاق على تبادل تسليم المجرمين بين الدول حول هذه الجرائم ضرورة ملحة[٤]، وهو ما نصت عليه اتفاقية بودابيست في المادة ٢٤ منها، حيث أكدت هذه المادة على ضرورة أن تلتزم الأطراف المتعاقدة بإدراج هذه الجرائم بوصفها جرائم تستوجب تسليم المجرمين.

وقد نظم المشرع مسألة تسليم المجرمين في قانون الإجراءات الجزائية من المواد ٦٩٤ إلى ٧٢٠، ومن بين ما جاء في هذه المواد أنه يجوز للحكومة الجزائرية أن تسلم شخصا غير جزائري إلى حكومة أجنبية بناءا على طلبها، إذ وجد في أراضي الجمهورية وكانت قد اتخذت في شأنه إجراءات متابعة باسم الدولة الطالبة أو صدر حكم ضده من محاكمها ولا يجوز تسليم المجرمين إلا إذا كانت الجريمة محل الطلب قد ارتكبت في أراضي الدولة الطالبة أو من رعاياها.

ويشترط المشرع الجزائري أن تكون الجريمة محل الطلب تشكل جناية أو جنحة تزيد عقوبتها عن سنتين، ولا يجوز التسليم في الحالات الأخرى إلا إذا كان المتهم قد

1– أوصت الاتفاقية الأوروبية للإجرام المعلوماتي بودابيست كل طرف تبني إجراءات تشريعية لأجل الوفاء بالالتزامات المتفق عليها في مجال التعاون الدولي، وأجازت لأي طرف في حالة الاستعجال أن يقدم طلبا للمساعدة المتبادلة... وفي المقابل أوجبت على الدول المقدم إليها الطلب أن توافق على الطلب أو على الأقل أن ترد عليه بأي وسيلة مستعجلة .

2– أنظر في هذا المعنى، شول بن شهرة، المرجع السابق، ص ٣٧٩.

3– وبالرجوع إلى اتفاقية بودابيست نجدها تنص على أنه يمكن للدول أن تضع بعض الشروط في قوانينها الداخلية أو في الاتفاقيات الدولية لتنظيم عملية تبادل المعلومات ونقل الإجراءات نذكر منها :

– أن يكون الاجراء المطلوب اتخاذه مقرر في القانون الداخلي للدولة المطلوب منها الاجراء وهو ما يعرف بشرعية الإجراء.

– أن يكون هذه الإجراء مناسب للوصول إلى الحقيقة المتعلقة بأدلة الجريمة المرتكبة.

– أن يكون الإجراء المطلوب اتخاذه بصدد نقل مجرم في الدولة المطلوب منها الإجراء وكذا الدولة الطالبة له.

4– أنظر، جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن الحاسب الآلي، الكتاب الأول، دار النهضة العربية، ط ١٩٩٢، ص ٩٠.

عوقب بالحبس لأكثر من شهرين عن جريمة سابقة في تلك الدولة... وعليه فإن تسليم المجرمين المتهمين بارتكاب أحد الجرائم الماسة بالمعاملات التجارية الإلكترونية متوقف على تكييف الدولة الطالبة لهذه الجرائم، وكان من الأفضل لو نص المشرع على أن تسليم المجرمين يشمل كافة الجرائم الواقعة في البيئة الإلكترونية كونها جرائم عابرة للحدود، كما يجب أن يكون هناك تنسيق وتوحيد بين التشريعات المختلفة للدولة فما يخص تسليم المجرمين.

١-أ) هذه المادة تنطبق على تبادل المجرمينبين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانينالدول الأطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب) إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمينفإن العقوبة الدنيا هي التي سوف تطبق.

٢-إن الجرائم المنصوص عليها في الفقرة (ا) من هذه المادة تعتبر قابلة لتسليم المجرمينالذين يرتكبونها في أية معاهدة لتسليم المجرمينقائمة بين الدول الأطراف.

٣- إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمينمن دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمينفيما يتعلق بالجرائم المذكورة في الفقرة (ا) من هذه المادة.

٤-الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمينيجب أن تعتبر الجرائم المذكورة في الفقرة (ا) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول[1].

الفرع الثاني : نحو تعاون دولي في مجال تكوين رجال العدالة الجزائية

لأنه ما من دولة يمكنها النجاح في مواجهة هذا الجيل الجديد من الإجرام - المعروف بالجرائم المعلوماتية أو جرائم الانترنيت- دون تعاون وتنسيق مع غيرها من الدول، كانت الدعوة إلى ضرورة وجود تعاون دولي ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب...، وإنما أيضا في مجال تكوين رجال العدالة، خاصة فيما يتعلق بالجانب التقني والوسائل المستحدثة في التحقيق، فتدريب الكوادر البشرية ليس بنفس المستوى في جميع الدول وإنما يختلف تبعا لتقدم الدولة من عدمه، ولو أمعنا النظر في بعض التشريعات الدولية أو الإقليمية لوجدنا أنها دعت وبصريح النص إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينه.

وبالنظر إلى الكثير من الدول خاصة تلك النامية منها لا تتوفر أجهزة العدالة لديها على التكوين الكافي لمواجهة الجرائم الواقعة في بيئة الأعمال الإلكترونية ومثيلاتها من الجرائم، وذلك لعدة عوامل أهمها الافتقار إلى البنية التحتية والعنصر البشري ذوي الخبرة، أو لأن نظامها القانوني قد أكل الدهر عليه وشرب، أو افتقارها لأي قوانين تتصدى بها لهذه النوعية من الجرائم .

وقد تم عقد عدة اجتماعات على الصعيد العربي لدراسة مسألة التدريب والتأهيل المناسبين لأعضاء الهيئات القضائية العربية، وقد نتج عن هذه الاجتماعات مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمى اتفاقية عمّان للتعاون العلمي بين المعاهد القضائية العربية والتى وقعت في ٩ إبريل ١٩٩٧م، كما تم عقد عدة ندوات ومؤتمرات متخصصة في مواجهة هذا النوع من الجرائم.

ومن مظاهر التعاون الدولي في مجال إصلاح وتطوير أجهزة العدالة تنظيم الدورات التدريبية للعاملين فيها، وهي تهدف إلى تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحة الجريمة المعلوماتية في الدول المختلفة من خلال تبادل الخبرات، وطرح موضوعات ومشكلات للتدارس المشترك، والتعرف على أحدث

1- وقد الفقرات الأخرى من المادة على ما يلي :
٥- يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين.
٦-يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي تمتد إليها اختصاصها بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقبا عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفين المتعاقدين وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلبا بالملاحقة مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم.
٧-أ) تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي في ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.
ب) تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائما.

التطورات في مجال الجريمة الإلكترونية وأساليب مكافحتها[1].

وتعتبر الولايات المتحدة الأمريكية من الدول الرائدة في هذا المجال فهي تحرص على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى، ومساعدة ما لديها من أجهزة شرطة، ومسئولي الإدعاء العام، والقضاة ليصبحوا أكثر فعالية في مكافحة الجرائم الواقعة في بيئة الأعمال الإلكترونية، حيث يتواجد لدى الولايات المتحدة الأمريكية مكتب مساعدة وتدريب وأجهزة الإدعاء العام في الخارج، وهو تابع لوزارة العدل الأميركية، مكلف تحديداً بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى، وتعزيز إدارة القضاء في الخارج، كما تقدّم وزارة العدل الأميركية مساعدات لتطوير القطاع القضائي في عدد من البلدان في أفريقيا، وآسيا، وأوروبا الشرقية والوسطى وأميركا اللاتينية ومنطقة حوض الكاريبتي، والدول المستقلة حديثاً، بما ذلك روسيا والشرق الأوسط، مستعينة في ذلك بخبرة الوحدات المتخصصة التابعة لها.

وعلى الرغم من أن المشرع الجزائري حاول تنظيم الجانب الإجرائي للجرائم الواقعة في البيئة الإلكترونية وذلك بموجب القانون رقم ٠٤/٠٩ المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام كما ذكرنا سابقا، إلا أنه لم يحدث جهة تختص بالجرائم الإلكترونية، مع أنه أشار إلى مسألة تفتيش المنظومات المعلوماتية في المادة ٥ من القانون ولكنه جعل الجهة المختصة به هي الجهات المنصوص عليها في القواعد العامة.

وتجتهد الحكومة الجزائرية في إطار مسايرتها للتطور التكنولوجي في تكوين فرق من الدرك والشرطة للبحث والتنقيب في مثل هذه الجرائم وذلك عن طريق إرسال بعثات إلى الخارج للتكوين في هذا المجال خاصة فرنسا، كما يتم عقد العديد من الندوات والأيام الدراسية حول ضرورة إحداث سلطة قضائية لهذا النوع من الجرائم المستحدثة.

كما أشار القانون رقم ٠٤/٠٩ السالف الذكر في مادته العاشرة إلى أنه يمكن للمكلفين بالتحريات القضائية الاستعانة بمقدمي خدمات[2]، من أجل جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها، وكل ذلك تحت تصرف ورقابة السلطات المختصة بالتحري والتحقيق[3]، كما فرض المشرع عدة التزامات على مقدمي خدمات الأنترنيت تتمثل في السحب الفوري لكل المعلومات التي يتيحون الإطلاع عليها والتي تكون محل حظر سواء تم ذلك بطريقة مباشرة أو غير مباشرة[4].

والى جانب مقدمي خدمات الأنترنيت أنشأ المشرع هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مهمتها تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريمها، بما في ذلك جمع المعلومات وإجراء الخبرة، كما تعمل الهيئة على تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذه الجرائم....، وقد أحال المشرع على التنظيم لبيان الهياكل البشرية والقاعدية لهذه الهيئة.

ورغم هذا تبقى تحركات الدولة الجزائرية في هذا المجال بطيئة جداً لا تتماشى مع تزايد الجرائم التى تقع على بيئة الأعمال الإلكترونية، سواء كانت تجارية أو غيرها، ولذلك يكون من الضروري الإسراع في تكوين فرق متخصصة للبحث والتحري في مثل هذه الجرائم.

خلاصة القول أنه لا يمكن لأي دولة مهما بلغت من التقدم والتطور أن تواجه هذه الأنماط المستحدثة من الجرائم لوحدها، ولذلك فلا مفر من تعزيز التعاون الدولي في الجانب الإجرائي، ثم لا مفر لهذه الدول من تقديم المساعدة للدول النامية لتعزيز مؤسساتها المتخصصة

1- وقد يتحقق ذلك عن طريق عقد اللقاءات وحلقات المناقشة المصغرة بين مسؤلي الاتصال بالسفارات أو المكاتب الإقليمية للمنظمات والأجهزة المعنية مع جهات أو أطراف لها علاقة، ويتم خلالها تبادل الآراء والخبرات بين المشاركين، وتمثل كافة هذه اللقاءات وحلقات المناقشة وسيلة فعّالة للحوار والمناقشة والتشاور للتعارف وتبادل الرأي والخبرة وطرح الأفكار والتصورات وتدارس سبل تنمية وتشجيع التعاون فيما بين الأطراف.

2- يعد مقدم خدمات حسب المادة الأولى من قانون ٠٤/٠٩ " كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات .

وكذلك أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها ".

3- ويتعين على مقدمي الخدمات في هذه الحالة كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك طائلة قانون العقوبات.... ينظر المادة ١٠ من القانون رقم ٠٤/٠٩.

4- كما يتوجب عليهم وضع الترتيبات التقنية التي تسمح بحظر إمكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام العام وللآداب العامة وإخبار المشتركين لديهم بوجودها... ينظر المادة ١٢ من القانون ٠٤/٠٩....ينظر أيضا... بن عبد الله الأزرق، نظام المعلوماتية في القانون الجزائري، المؤتمر السادس حول البيئة المعلوماتية الآمنة، جمعية المكتبات والمعلومات، السعودية، الرياض، ٢٠١٠، ع م .

بالتحري والتحقيق والمحاكمة، وذلك من خلال توفير التدريب التكوين والوسائل اللازمة.

٢. الخاتمة :

إنّ المتمعّن في تجربة الجزائر في مجال مكافحة الجريمة المعلوماتية ،يجد نوعا من التباين بين نوعي الحماية فقد اكتفى المشرّع بسن بعض النصوص القانونية ضمن قانون العقوبات في محاولة لمواجهة الجرائم المعلوماتية والإلكترونية بصفة عامة، كتجريم الدخول أو البقاء داخل نظام المعالجة وكذا المساس غير العمدي بسير نظام المعالجة، بالإضافة إلى تجريم المساس بالمعلومات داخل نظام المعالجة، في حين نجد أن أنه أغفل تجريم بعض صور الجرائم المعلوماتية الأخرى مثل المساس العمدي بسير نظام المعالجة والجرائم المتعلقة بالمعلومات الشخصية مثل :

- جريمة عدم الاتخاذ الإجراءات الأولية لإجراء معالجة البيانات.
- جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة.
- جريمة المعالجة غير المشروعة للبيانات.
- جريمة تسجيل وحفظ بيانات شخصية أو تتعلق بالماضي لأشخاص مصنفين.
- جريمة حفظ شخصية خارج الوقت المخصص به وفقا للطالب.
- جريمة تغيير الغرض المحدد لجمع البيانات الاسمية.
- جريمة إفشاء بيانات إسمية إضرار بصاحب الشأن.

ومن هنا ندعو المشرع وباقي التشريعات إلى سن قانون خاص لمكافحة الجريمة المعلوماتية، وتكون الاتفاقية العربية لمكافحة جرائم تقنية المعلومات مصدرا لهذا القانون حتى يكون هناك نوعا من التوافق بين القوانين العربية ، ومن هنا أيضل نثمن مصادقة المشرع على هذه الاتفاقية في انتظار إصدارها في شكل قانون خاص.

أما في الجانب الإجرائي فقد أحسن المشرع بنصه على القانون رقم ٠٩/٠٤ والمتعلق بالوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها، في انتظار تدعيم هذا القانون بالإجراءات الجديدة التي تناولتها الاتفاقية العربية السالفة الذكر، ويكون من الأفضل لو ضمن المشرع هذا القانون ضمن قانون خاص يجرم الأفعال الماسة بالمعلومات وينظم إجراءات المتابعة والتحقيق فيها .

ومن هنا أيضا ندعو الحكومة الجزائرية وباقي الحكومات العربية والعالمية للتعاون في سبيل تكوين رجال مختصين في البحث والتحقيق في مثل هذه الجرائم

.

٣. ملخص النتائج والتوصيات :

النتائج :

١. إنّ المشرّع الجزائري وُفق إلى حد كبير وضع نصوص قانونية لمكافحة الجريمة الإلكترونية رغم أنه لم يسن قانون خاص لذلك.
٢. أن المشرع الجزائري صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
٣. أن المشرع الجزائري نص على قانون خاص ولا مثيل له في الدول العربية وهو القانون المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها وهو قانون إجرائي وليس موضوعي.

التوصيات :

١. ضرورة المصادقة على الاتفاقية العربية لمكافحة الجريمة الإلكترونية.
٢. ضرورة التعاون الدولي في مجال توحيد نصوص التجريم في المجال الإلكتروني.
٣. ضرورة التعاون الدولي في مجال تكوين أجهزة مختصة في مكافحة الجريمة الإلكترونية.
٤. ضرورة استقطاب هذا النوع من المجرمين ومحاولة الاستفادة من خبراتهم.
٥. ضرورة اعتماد نظام المرشد الجنائي وفتح مواقع لتلقي الشكاوى لتسهيل عملية القبض على هؤلاء المجرمين.
٦. ضرورة تكثيف الدراسات حول طبيعة المجرم المعلوماتي، ونرى أنه حان الوقت لميلاد علم جديد وهو علم الإجرام المعلوماتي.

المراجع

المصادر:

[١] قانون العقوبات الجزائري

[٢] القانون رقم ٠٩-٠٤، الصادر بتاريخ ٥ أوت ٢٠٠٩ ج ع ٤٧.

[٣] اتفاقية بودابيست للإجرام المعلوماتي لسنة ٢٠٠١.

المراجع:

[٤] أسامة أحمد المناعسة، جرائم الحاسب الآلي و الانترنيت، دار وائل، ط١، عمان، ٢٠٠١.

[٥] أمال قارة، الحماية الجنائية للمعلوماتي في التشريع الجزائري، دار هومة للنشر، ط ٢٠٠٧.

[٦] بن عبد الله الأزرق، نظام المعلوماتية في القانون الجزائري، المؤتمر السادس حول البيئة المعلوماتية الآمنة، جمعية المكتبات والمعلومات، السعودية، الرياض، ٢٠١٠.

[٧] خثير مسعود، الحماية الجنائية لبرامج الحاسب الآلي، مذكرة ماجستير، كلية الحقوق، جامعة أبي بكر بلقايد تلمسان، ٢٠٠٨.

[٨] خليفة محمد، جريمة التواجد غير المشروع في الأنظمة المعلوماتية، رسالة دكتوراه كلية الحقوق جامعة باجي مختار عنابة، ٢٠١٠/٢٠١١.

[٩] رامي عبد الحليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجموعة الملتقى الدولي حول التنظيم القانوني للانترنيت...، مجلة دراسات، ٢٠٠٩.

[١٠] سليم عبد الله الخيوري، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية، ط١، ٢٠١١.

[١١] شول بن شهرة، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، جامعة محمد خيضر بسكرة، ٢٠٠٩/٢٠١٠ .

[١٢] عبد الغني محمد عطالله، الحماية الجنائية للتعاملات الالكترونية، دار الجمعة الجديدة، ٢٠٠٧.

[١٣] عبد الفتاح بيومي حجازي، الحماية الجنائية لنظام، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤.

[١٤] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي في جرائم الكمبيوتر والانترنيت، دار الكتب القانونية مصر، ط١، ٢٠٠١.

[١٥] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، الدار الجامعية للطباعة والنشر، بيروت، ١٩٩٩.

[١٦] محمد أحمد طه، المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٣.

[١٧] هلالي عبد الإله أحمد، اتفاقية بودابست لمكافحة جرائم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٧.

[١٨] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن الحاسب الآلي، الكتاب الأول، دار النهضة العربية، ط ١٩٩٢، ص ٩٠.

[١٩] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات

Summary

Cybercrimes can be summarized in any unlawful behavior that interferes with electronic processes that affect electronic systems of information and security of processed data.

These crimes have reversed the balance of criminalization and punishment for not acting against tangible physical behavior but acts made in the virtual world and the regular inquiry mechanisms are no longer sufficient as there is no physical strength or combat skills but the knowledge and control of information. The investigator must therefore know the information technology and media and communications requirements, helping to arrest the criminal.

In light of the proliferation of electronic crimes and the diversity of models and methods, research bodies and competent investigation, including the judicial police are unable to keep pace with this development and the investigation of this type of crime. This has led many countries to resort to the creation of competent bodies which can cope with this type of crime.

The reason for the current study

The legislator faces various crimes by the criminalization and punishment as a kind of purpose and control to identify these crimes and arrest criminals, it provides the necessary human and material resources as a sort of procedural control. This remains normal and without a problem as long as it is concerns traditional crimes, but it's different when one faces unusual crimes, crimes taking place in a virtual world.

It is the deficit of the rules of substance and procedure to pursue this type of crimes that motivates this study, which aims to develop

technologies, a procedural law and not an objective one.

Recommendations

1. The need for the ratification of the Arab Convention for the fight against cybercrime.
2. The need for international cooperation in the field of standardization of criminal provisions in the electronic field.
3. The need for international cooperation in the field of establishment of relevant bodies in the fight against electronic crime.
4. The need to attract these criminals and try to benefit from their expertise.
5. The need for criminal advisor system and open sites to receive complaints to facilitate the arrest of these criminals.
6. The need to intensify research on nature of criminal information and we believe it is time to create a new science, the information criminology.

Keywords—Electronics; virtual; crime; substance; procedure; computing; system

solutions able to ensure the intervention of criminal law in the field of the virtual world.

The methodology

In order to achieve the desired outcomes and recommendations, we opt for the analytical method to try to analyze the existing legal texts and the descriptive method to try to describe the phenomenon of crime and define its dimensions and relatively, the comparative approach particularly in regard of the Budapest Convention and the Arab Convention for the Prevention of information technology crimes.

The results and recommendations

The results

1. The Algerian legislature, has to a large extent, succeeded in the development of legal texts in the fight against cybercrime, even if it has not passed a special law to do so.
2. The Algerian Parliament has ratified the Arab Convention for the Prevention of Information Technology Crimes.
3. The Algerian legislature has provided an unprecedented special law in the Arab countries, a law on the prevention and fight against crimes of information and communication